● 国家出版基金资助项目

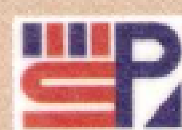
中国科学院华罗庚数学重点实验室丛书

华罗庚文集

数论卷 I

华罗庚 /著

王 元 /审校



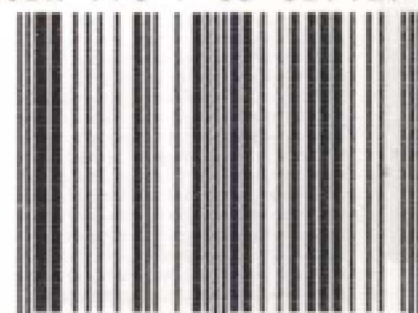
科学出版社

www.sciencep.com

(O-3860.0101)

中国科学院华罗庚数学重点实验室丛书

华罗庚文集 | 数论卷 I |



ISBN 978-7-03-027127-3

9 787030 271273 >

销售分类建议：高等数学

定 价：98.00元

国家出版基金资助项目

中国科学院华罗庚数学重点实验室丛书

华罗庚文集

数论卷 I

华罗庚　著

王　元　审校

科学出版社

北　京

内 容 简 介

本书分两部分，上部为堆垒素数论；下部为指数和的估计及其在数论中的应用.

第一部分是关于堆垒素数论方面苏联维诺格拉陀夫院士的研究方法和作者自己的研究方法的总结性论著. 在这部分中给予维诺格拉陀夫院士的中值定理以显著的中心地位，并且改进了它. 作者把华林问题与哥德巴赫问题的研究方法结合起来，并把华林问题一方面推广到每一加数是整系数多项式的情形，一方面限制变数仅取素数值. 作者把塔锐问题也加上了变数只取素数值的限制，同时又讨论到更广的素未知数的不定方程组.

下部主要讨论了指数和的各种估计方法及其应用，特别讨论了这些方法对 Waring 问题及 Гольдбах问题的应用. 除此而外，也谈到了解析数论的其他一些问题与方法. 这部分不仅综合了这几方面的结果与文献，更重要的是对其中绝大部分重要的结果都给出了较完备的提纲性的证明.

本书适合数学及相关专业大学生、研究生、教师及科研人员阅读参考.

图书在版编目(CIP)数据

华罗庚文集：数论卷 I/华罗庚著；王元审校. —北京：科学出版社，2010

(中国科学院华罗庚数学重点实验室丛书)

ISBN 978-7-03-027127-3

Ⅰ.华… Ⅱ.华… Ⅲ.①数学-文集 ②数论-文集 Ⅳ.01-53

中国版本图书馆 CIP 数据核字(2010) 第 056714 号

责任编辑：张 扬／责任校对：陈玉凤

责任印制：钱玉芬／封面设计：黄华斌

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

中国科学院印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2010 年 5 月第 一 版 开本：B5(720×1000)

2010 年 5 月第一次印刷 印张：21 1/2

印数：1—3 000 字数：393 000

定价：98.00 元

(如有印装质量问题，我社负责调换)

纪念华罗庚先生诞辰100周年

《华罗庚文集》编委会

《华罗庚文集》序言

2010 年是著名数学家华罗庚先生诞辰 100 周年. 值此机会, 我们编辑出版《华罗庚文集》, 作为对他的美好纪念.

华罗庚先生是他那个时代的国际领袖数学家之一, 也是中国现代数学的主要奠基人和领导者. 无论是在和平建设时期, 还是在政治动荡甚至是战争年代, 他都抱定了为国家和人民服务的宗旨, 为中国数学的发展倾注了毕生精力, 受到了中国人民的广泛尊敬.

华罗庚先生最初研究数论, 后将研究兴趣拓展至代数和多复变等多个领域, 取得了一系列国际一流的成果, 引领了这些领域的学术发展, 产生了广泛持久的影响. 他从一名自学青年成长为著名数学家, 其传奇经历激励了几代中国数学家投身于数学事业.

华罗庚先生为我们留下了丰富的精神遗产, 包括大量的学术著作和研究论文. 我们认为, 认真研读这些著作和论文, 是深刻把握华罗庚学术思想精髓的最佳途径. 无论对于数学工作者还是青年学生, 其中许多内容都是很有启发和裨益的.

华罗庚先生担任中国科学院数学研究所所长 30 余年, 他言传身教, 培养和影响了一批国际水平的数学家, 他的学术思想和治学精神已经成为数学所文化的核心. 自 2008 年起以中科院数学所为基础成立的中国科学院华罗庚数学重点实验室, 旨在继承和弘扬华罗庚先生的学术思想和治学精神, 积极推动中国数学的发展. 为此, 我们选择华罗庚先生的著作和论文作为实验室的首批出版物, 今后还将陆续推出更多优秀的数学出版物.

在出版《华罗庚文集》的过程中, 我们得到了各方面的关心和支持, 包括国家出版基金的资助, 在此我们表示深深的感谢. 同时, 对于有关人员在策划、翻译和审校等方面付出的辛勤劳动, 对于科学出版社所作的大量工作, 我们表示诚挚的谢意.

中国科学院华罗庚数学重点实验室

《华罗庚文集》编委会

2010 年 3 月

目　录

华罗庚文集数论卷 I · 上部

华罗庚文集数论卷 I · 下部

（华罗庚文集数论卷 I · 上部）

堆垒素数论[1]

[1] 本部分内容曾作为著作出版，见《堆垒素数论》，北京：科学出版社，1957 年.

谨以此书祝中苏邦交永笃[1]

华罗庚
1941年2月18日

В ЗНАК ВЕЧНОЙ ДРУЖБЫ
МЕЖДУ
КИТАЕМ И СССР
С ГЛУБОКИМ УВАЖЕНИЕМ

АВТОР

---

① 取自《堆垒素数论》.

再 版 序[①]

作者利用这一次再版的机会对本书做了一些修改和补充. 第 4 章第 5 节、第 5 章第 6 节和第 8 节及第 9 章全部都是经过重写的, 此外还有不少章节做了部分改写工作.

读者读了本书后, 再参阅不多的近代文献, 如不久将在数学学报上发表的作者论文 “堆垒数论上的一些结果”, 就可以了解近代堆垒数论的中心部分, 并且可以进入研究工作的领域. 但不要忘记, 本书只是一个专著, 仅仅是叙述了数论中的一个分支, 在深入的同时, 也应当去了解数论的宽广园地 (请参阅科学出版社出版的拙著 “数论导引”).

作者乘此机会向越民义、王元、吴方、魏道政、陈景润诸的同志表示谢意, 他们或指出错误或给以帮助, 不是他们的协同工作, 再版是不会这样快就问世的.

华罗庚

1957 年 7 月 7 日于北京

---

① 取自《堆垒素数论》

序 ①

这一本小书能够用本国文字出版是和人民民主政权分不开的. 回忆一下离初稿完成的日子已经过了十二个年头了, 离俄文版刊出的日子也已隔了六年了. 在解放以前漫长的岁月中, 这书在我国刊出的问题, 由即将出版、等待出版一直演变到把原稿搞得无影无踪, 以至于到了今天, 在中国科学院敦促之下我还得从俄文本翻译出来付印. 这些事实, 有力地说明了, 旧政权是怎样腐化怎样地不关心科学, 而人民民主政权又是怎样地宝爱科学成果.

十二个年头不算短暂, 科学工作又有了不少的进展, 所以仅把俄文本翻译付印, 是不合当前的情况的. 我改写了几章, 特别是第 5 章我把维诺格拉陀夫院士在 1942 年到 1947 年进一步的创造性的工作及著者 1947 年的工作包括进去.

在工作完成的时候, 心情是异常愉快的. 不但由于我的小书得以在祖国出版, 而特别是从前所渴望着的中苏两国的友谊今天是实现了 —— 已经牢不可破了! 没有中国科学院的鼓励, 这本书是不可能再出版的, 所以我由衷地表示感谢. 数学研究所的同人分头负责核阅及订正, 人数之多使我不能在这儿一一列举. 只有在集体主义的今天才会出现这样友爱团结的精神. 而这又证明了人民民主政权的优越性.

华罗庚

1953 年 5 月于北京

① 取自《堆垒素数论》

俄文版原序[1][2]

本文中叙述了关于堆垒素数论的新结果, 这一学科的基础是由И. М.维诺格拉陀夫院士所奠立的, 而由著者发展的. 在第 5、6 两章把开拓了新途径的维诺格拉陀夫院士的工作加以简化与改变而重述出来. 阅读本文, 除了引理 7.14 之外, 并不要求有任何其他较专门化的知识.

本文中大部分是著者所获得并在这里首次发表的结果的系统叙述.

无论著者如何地感谢维诺格拉陀夫院士都不会是过分的.

闵嗣鹤、钟开莱两位先生对于本文手稿之准备都曾给予帮助.

最后, 著者对苏联科学院对他的著作的好评价愿表示深切的谢意. 在这些困难的日子里, 我们的科学研究的成果能获得最友好的人民的最高权威方面的赞助, 这特别给予我们很大的鼓舞. 这种文化的合作是永远宝贵的, 而在现在的时刻, 这更具有特殊的意义. 谨祝此书的出版将会加强我们两国伟大人民间的真诚友谊与相互亲善.

华罗庚

中国昆明国立清华大学

1941 年 2 月 18 日

在几年的战争之后, 承维诺格拉陀夫院士给予我访问苏联的机会. 我非常高兴地获悉我在 1940—1941 年所写的这篇论文已在付印. 在 1942 年维诺格拉陀夫院士已把他的方法更精密化, 而著者在到莫斯科之前还完全不知道. 他的精密化加强了关于平均值的定理 (本文中的定理 7). 藉助这一定理我们可以改进定理 8, 9, 11, 13, 17 等等. 例如定理 11 对于 $s \geqslant 10k^2 \log k$ 也真实, 而定理 13 对于 $s \geqslant s_0 \sim 4k \log k$ 也正确, 等等.

最后, 我谨向翻译此文的Б. И. Сегал与Д. А. Басильков两位教授致谢.

华罗庚

莫斯科, 1946 年 4 月 17 日

① 编者 (指斯切克洛夫数学研究所专刊的编者) 识: 本书于 1941 年交数学研究所专刊编辑部, 但由于 1941—1945 年的战时条件, 现在才能出版.

② 取自《堆垒素数论》.

说　　明 [①]

本文并无一般的引言. 各章的第一段有主要结果的叙述. 本文中常引用下列符号:

对于实数 z, $[z]$ 表示不大于 z 的最大整数, 而 $\{z\}$ 表示由 z 到最近整数的距离.

$$e(z) = \mathrm{e}^{2\pi \mathrm{i} z}, \quad e_q(x) = \mathrm{e}^{2\pi \mathrm{i} x/q}.$$

k 表示一正整数; P 是充分大的正数, 而 $L = \log P$.

$\max(a, b, \cdots, g)$ 表示 $a, b, \cdots, g$ 中最大的一个, 而 $\min(a, b, \cdots, g)$ 表示其中最小的一个.

如习常所用: $a|b$ 表示 a 整除 b, $a \nmid b$ 表示 a 不整除 b. 本文中常用 p 表示素数, $p^l \| n$ 表示 $p^l | n$ 而 $p^{l+1} \nmid n$.

$c(a, b, \cdots, g)$ 表示某一依存于 $a, b, \cdots, g$ 的正数; ε 是任意小正数, 但不一定在每次出现时都是一样的.

$f(x) = O(\varphi(x))$ 或 $f(x) \ll \varphi(x)$ 表示

$$|f(x)| \leqslant c(a, b, \cdots, g)\varphi(x).$$

在陈述定理时我们不用符号 $\ll$ 及 O, 而用如以上形式的不等式. 在证明中或引理中如果用到符号 $\ll$ 或 O, 则其所包有的常数仅依赖于定理叙述中所涉及的 $a, b, \cdots, g$.

如有特别声明, 符号的含义可能有局部性的改变.

---

① 取自《堆垒素数论》.

第 1 章　三　角　和

§1.1　定理及基本引理的叙述

定理 1　命 $f(x)$ 代表一个有整数系数的多项式

$$f(x) = a_k x^k + \cdots + a_1 x + a_0.$$

若 $(a_k, \cdots, a_1, q) = 1$, 则

$$\left|\sum_{x=1}^{q} \mathrm{e}^{2\pi \mathrm{i} f(x)/q}\right| \leqslant c_1(k, \varepsilon) q^{1-\frac{1}{k}+\varepsilon},$$

此处 ε 是一任与的正数.

为了简单起见, 我们引用下面的符号:

$$a = \frac{1}{k}, \quad \mathrm{e}_q(x) = \mathrm{e}^{2\pi \mathrm{i} x/q}$$

及

$$S(q, f(x)) = \sum_{x=1}^{q} \mathrm{e}_q(f(x)).$$

基本引理 (引理 1.1)　若 $p \nmid (a_k, \cdots, a_1)$, 则

$$|S(p^l, f(x))| \leqslant c_2(k) p^{l(1-a)}.$$

§1.2　由基本引理推出定理

引理 1.2　用 $v(q)$ 表示 q 的不同的素数因子的个数. 用 $d(q)$ 表 q 的正除数的个数. 则

$$2^{v(q)} \leqslant d(q) \leqslant c_3(\varepsilon) q^{\varepsilon}.$$

证　若素数 $p > 2^{1/\varepsilon}$, 则

$$\frac{d(p^l)}{p^{l\varepsilon}} = \frac{l+1}{p^{l\varepsilon}} \leqslant \frac{l+1}{2^l} = \frac{l+1}{(1+1)^l} \leqslant \frac{l+1}{l+1} = 1.$$

又若素数 $p \leqslant 2^{l/\varepsilon}$ 及 $l \geqslant 1$, 则

$$\frac{d(p^l)}{p^{l\varepsilon}} = \frac{l+1}{p^{l\varepsilon}} \leqslant \frac{l+1}{2^{l\varepsilon}} \leqslant \frac{l+1}{l\varepsilon \log 2} \leqslant \frac{2}{\varepsilon \log 2}.$$

命 $q = p_1^{l_1} \cdots p_s^{l_s}$, 此处 $p_1, \cdots, p_s$ 是 q 所有的不同的素因子, 则

$$\frac{d(q)}{q^\varepsilon} = \prod_{p|q} \frac{d(p^l)}{p^{l\varepsilon}} \leqslant \prod_{p \leqslant 2^{1/\varepsilon}} \frac{2}{\varepsilon \log 2} = c_3(\varepsilon).$$

引理中第一不等式显然真实.

引理 1.3　若 $(q_1, q_2) = 1$ 及 $f(0) = 0$, 则

$$S(q_1 q_2, f(x)) = S(q_1, f(q_2 x)/q_2) S(q_2, f(q_1 x)/q_1).$$

证　命 $x = q_1 y + q_2 z$. 当 y 及 z 各经过以 q_2 及 q_1 为模的完全剩余系, 则 x 经过以 $q_1 q_2$ 为模的完全剩余系. 显然得出

$$e_{q_1 q_2}(f(q_1 y + q_2 z)) = e_{q_2}(f(q_1 y)/q_1) e_{q_1}(f(q_2 z)/q_2)$$

及

$$\begin{aligned} S(q_1 q_2, f(x)) &= \sum_{x=1}^{q_1 q_2} e_{q_1 q_2}(f(x)) \\ &= \sum_{y=1}^{q_2} \sum_{x=1}^{q_1} e_{q_2}(f(q_1 y)/q_1) e_{q_1}(f(q_2 z)/q_2) \\ &= S(q_1, f(q_2 x)/q_2) S(q_2, f(q_1 x)/q_1). \end{aligned}$$

定理的证明　我们可以假定 $a_0 = 0$ 而不失其普遍性. 命 $q = p_1^{l_1} \cdots p_s^{l_s}$, 此处 $p_1, \cdots, p_s$ 是 q 所有的不同的素因子. 由引理 1.3

$$S(q, f(x)) = \prod_{p|q} S\left(p^l, \frac{f(qx/p^l)}{q/p^l}\right)$$

及由引理 1.1 可得

$$|S(q, f(x))| \leqslant c_2^{v(q)} q^{1-a}.$$

再由引理 1.2(我们可设 $c_2 > 1$),

$$c_2^{v(q)} = (2^{v(q)})^{\log c_2/\log 2} \leqslant c_1(k, \varepsilon) q^\varepsilon.$$

由此即得出本定理.

§1.3　当 $l = 1$ 时基本引理的证明 (Mordell*)

并不失去普遍性, 我们可以假定 $p > k$ 及 $a_0 = 0$. 为了简单起见, 我们用 $\sum_x$ 代表 $\sum_{x=1}^{p}$. 如是得到

$$\begin{aligned}&\sum_{a_k}\cdots\sum_{a_1}\left|\sum_x e_p(a_kx^k+\cdots+a_1x)\right|^{2k}\\=&\sum_{x_1}\cdots\sum_{x_k}\sum_{y_1}\cdots\sum_{y_k}\sum_{a_k}\cdots\sum_{a_1}e_p(a_k(x_1^k+\cdots+x_k^k-y_1^k-\cdots-y_k^k)\\&+\cdots+a_1(x_1+\cdots+x_k-y_1-\cdots-y_k))=p^kN,\end{aligned}$$

此处 N 表示下列相合式组的解答的个数:

$$x_1^h+\cdots+x_k^h\equiv y_1^h+\cdots+y_k^h \pmod p,\quad 1\leqslant h\leqslant k,\ 1\leqslant x,\ y\leqslant p. \tag{1}$$

注意, 获得此结论时, 引用了下面的公式

$$\sum_{x=1}^{q}e_q(hx)=\begin{cases}q, & 若\ q|h,\\ 0, & 若\ q\nmid h.\end{cases}$$

由对称函数中一习知的定理, 由 (1) 可以引出

$$(x-x_1)\cdots(x-x_k)\equiv(x-y_1)\cdots(x-y_k)\pmod p.$$

由此可知 $y_1,\cdots,y_k$ 乃由 $x_1,\cdots,x_k$ 转换次序而得出的 (mod p). 所以

$$N\leqslant k!p^k.$$

由此得出

$$\sum_{a_k}\cdots\sum_{a_1}|S(p,a_kx^k+\cdots+a_1x)|^{2k}\leqslant k!p^{2k}. \tag{2}$$

显然, 对任一 $\lambda(\not\equiv 0 \pmod p)$ 及任一 μ 常有

$$|S(p,f(x))|=|S(p,f(\lambda x+\mu)-f(\mu))|.$$

所有这种形式的和都在 (2) 式的左边出现. 今往求出由所有不同的多项式 $f(\lambda x+\mu)-f(\mu)$ 所得的和 $S(p,f(\lambda x+\mu)-f(\mu))$ 的个数. 若二多项式的系数各各相合

* *Quarterly Jour. of Math.*, 3(1932), 161—167.

(mod p), 则此二多项式算为全同, mod p. 我们可以假定 $p \nmid a_k$ 而不失其普遍性. 若 $f(\lambda x+\mu)-f(\mu)$ 与 $f(x)$ 全同, mod p, 则得

$$a_k\lambda^k \equiv a_k, \quad ka_k\lambda^{k-1}\mu + a_{k-1}\lambda^{k-1} \equiv a_{k-1} \pmod p.$$

适合 $\lambda^k \equiv 1 \pmod p$ 的 λ 的个数 $\leqslant k$. 对一固定的 λ, μ 就唯一决定. 所以形如 $f(\lambda x+\mu)-f(\mu)$ 的多项式中最多有 k 个与 $f(x)$ 全同, mod p.

由此可得, 在所有的 $p(p-1)$ 个多项式

$$f(\lambda x+\mu)-f(\mu), \quad 1 \leqslant \lambda \leqslant p-1,\ 1 \leqslant \mu \leqslant p$$

中, 至少有 $p(p-1)/k$ 个是互不相同的. 所以

$$ap(p-1)|S(p,f(x))|^{2k} \leqslant k!p^{2k},$$

即

$$|S(p,f(x))| \leqslant \left(\frac{k\cdot k!}{p(p-1)}\right)^{\frac{1}{2}a} p \leqslant (2k\cdot k!)^{\frac{1}{2}a}p^{1-a} \leqslant kp^{1-a}. \tag{3}$$

§1.4 几条引理

引理 1.4　假定 $s(x)$ 是一整数系数的多项式, mod $p.\alpha$ 是 $s(x)\equiv 0 \pmod p$ 的 m 重根. $p^u \| s(px+\alpha)^*$. 命 $t(x)=p^{-u}s(px+\alpha)$, 则相合式

$$t(x) \equiv 0 \pmod p$$

至多有 m 个根.

证　并不失其普遍性, 可以假定 $\alpha=0$. 如此则

$$s(x)=x^m s_1(x)+ps_2(x),$$

此处 $s_1(0)\not\equiv 0 \pmod p), s_2(x)$ 的次数低于 $m.s_1(x)$ 及 $s_2(x)$ 都是整系数多项式. 由此得出

$$s(px)=p^m x^m s_1(px)+ps_2(px).$$

因为 x^m 的系数 $p^m s_1(0)$ 不能为 p^{m+1} 所整除, 所以 $u\leqslant m$. 又因为 $p^{-u}s(px)$ 的次数 $\leqslant m \pmod p$, 所以证明了本引理.

引理 1.5　假定

$$f(x)=a_kx^k+\cdots+a_1x,$$

* $p^u\|g(x)$ 表示 p^u 整除 $g(x)$ 的所有的系数, 但 p^{u+1} 不能.

$p \nmid (a_k, \cdots, a_1)$. 如果 p^σ 恰能整除 $f(\mu + py) - f(\mu)$ 所有的系数, 则

$$1 \leqslant \sigma \leqslant k.$$

证　假定 $\sigma \geqslant k+1$, 则由于 p^σ 能整除 $f(\mu+py)-f(\mu)$ 所有的系数, 可知

$$p^\sigma \left| \frac{p^h}{h!} f^{(h)}(\mu), \quad 1 \leqslant h \leqslant k, \right.$$

即对任一 h 常有

$$p^{k+1} \left| \frac{p^h}{h!} f^{(h)}(\mu), \right.$$

由此得出

$$p \left| \frac{1}{h!} f^{(h)}(\mu). \right.$$

因而得出 $p|a_k, p|a_{k-1}, \cdots, p|a_1$. 此与假定 $p \nmid (a_k, \cdots, a_1)$ 相违背.

§1.5　基本引理的证明

基本引理可以由以下的更明确的引理来概括.

引理 1.6　命 $f(x) = a_k x^k + \cdots + a_1 x + a_0, p \nmid (a_k, \cdots, a_1)$. 则

$$|S(p^l, f(x))| \leqslant k^3 p^{(1-a)l}.$$

证　命 t 是能整除 $(ka_k, \cdots, 2a_2, a_1)$ 的 p 的最高方次. 又设 $\mu_1, \cdots, \mu_r$ 是相合式

$$f'(x) \equiv 0 \pmod{p^{t+1}}, \quad 0 \leqslant x < p$$

的相异的根. 其重数分别为 $m_1, \cdots, m_r$. 命 $m_1 + \cdots + m_r = m$, 易见 $m \leqslant k-1$. 此引理显然是不等式

$$|S(p^l, f(x))| \leqslant k^2 \max(1, m) p^{(1-a)l} \tag{4}$$

的直接推理. 现在用数学归纳法来证明上式.

由于 $p \nmid (a_k, \cdots, a_1)$ 及 $p^t \| (ka_k, \cdots, 2a_2, a_1)$, 所以一定有 $p^t \leqslant k$.

1) 假定 $l < 2(t+1)$. 如果 $t = 0$, 即得 $l = 1$. 这是已经讨论过的情况. 若 $t \geqslant 1$, 则显然可见

$$|S(p^l, f(x))| \leqslant p^l \leqslant p^{l(1-a)} \cdot p^{(2t+1)a} \leqslant p^{l(1-a)} k^{(2+1/t)a} \leqslant k^2 p^{l(1-a)},$$

故引理成立.

2) 假定 $l \geqslant 2(t+1)$. 写

$$S(p^l, f(x)) = \sum_{v=1}^{p} \sum_{\substack{0 \leqslant x \leqslant p^l - 1 \\ x \equiv v \pmod p}} e_{p^l}(f(x)) = \sum_{v=1}^{p} S_v.$$

如果 v 并非 μ_i 之一, 则命

$$x = y + p^{l-t-1}z, \quad 0 \leqslant y < p^{l-t-1},\ 0 \leqslant z < p^{t+1},$$

即得

$$\begin{aligned} S_v = \sum_{\substack{0 \leqslant x < p^l \\ x \equiv v \pmod p}} e_{p^l}(f(x)) &= \sum_{\substack{0 \leqslant y < p^{l-t-1} \\ y \equiv v \pmod p}} \sum_{0 \leqslant z < p^{t+1}} e_{p^l}(f(y) + y^{l-t-1} z f'(y)) \\ &= \sum_{\substack{0 \leqslant y < p^{l-t-1} \\ y \equiv v \pmod p}} e_{p^l}(f(y)) \sum_{z=0}^{p^{t+1}-1} e_{p^{t+1}}(z f'(y)) = 0, \end{aligned} \tag{5}$$

最后等式是由于 $f'(y) \not\equiv 0 \pmod{p^{t+1}}$.

如果 $v = \mu_i$, 则依引理 1.5 来定义 σ_i, 如此则得

$$\begin{aligned} S_{\mu_i} = \sum_{\substack{x=1 \\ x \equiv \mu_i \pmod p}}^{p^l} e_{p^l}(f(x)) &= \sum_{y=1}^{p^{l-1}} e_{p^l}(f(\mu_i + py)) \\ &= e_{p^l}(f(\mu_i)) \sum_{y=1}^{p^{l-1}} e_{p^{l-\sigma_i}}(p^{-\sigma_i}(f(\mu_i + py) - f(\mu_i))). \end{aligned}$$

命 $g_i(x) = p^{-\sigma_i}(f(\mu_i + px) - f(\mu_i))$. 由引理 1.5 可知

$$\begin{aligned} |S_{\mu_i}| &= p^{\sigma_i - 1} |S(p^{l-\sigma_i}, g_i(x))| \\ &\leqslant p^{\sigma_i(1-a)} |S(p^{l-\sigma_i}, g_i(x))|. \end{aligned} \tag{6}$$

总括 (5), (6) 二式得出

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} p^{\sigma_i(1-a)} |S(p^{l-\sigma_i}, g_i(x))|. \tag{7}$$

如果 $l > \max(\sigma_1, \cdots, \sigma_r)$, 即用归纳法并引理 1.4, 由 (7) 式可得

$$|S(p', f(x))| \leqslant \sum_{i=1}^{r} m_i p^{\sigma_i(1-a)} k^2 p^{(l-\sigma_i)(1-a)} < m k^2 p^{l(1-a)}.$$

若 $l \leqslant \max(\sigma_1, \cdots, \sigma_r)$, 则 $l \leqslant k$

$$|S(p^l, f(x))| \leqslant \sum_{i=1}^{r} p^{\sigma_i - 1} p^{l-\sigma_i} \leqslant kp^{l(1-a)}.$$

由是基本引理即已完全证明.

所以定理 1 也就已经完全证明.

§1.6　推　　论

在论述若干推理之前, 我们先引入关于整值多项式的观念.

定义　如果对整数 x, 一多项式 $f(x)$ 的值也是整数, 这多项式就称为整值多项式.

引理 1.7　命

$$v!F_v(x) = x(x-1)\cdots(x-v+1).$$

一多项式是整值多项式的必要且充分条件是它可以表成

$$a_kF_k(x) + \cdots + a_1F_1(x) + a_0$$

的形式, 此处 $a_k, \cdots, a_1, a_0$ 都是整数.

证　显然 $F_v(x)$ 是整值多项式, 所以 $a_kF_k(x) + \cdots + a_1F_1(x) + a_0$ 也是整值多项式.

反之, 任一多项式常可表成

$$f(x) = b_kF_k(x) + \cdots + b_1F_1(x) + b_0.$$

连续以 $x = 0, 1, 2, \cdots, k$ 代入上式, 若 $f(x)$ 为整值多项式, 则可知诸 b 一定是整数.

现在可叙述本章的定理及基本引理的推论.

推论 1.1　命 $f(x)$ 是一 k 次整值多项式, 它的系数的最小公分母用 d 表示. 设 $p^t \| d$, 并且假定并非 $f(x)$ 的所有的非常数项的系数的分子都是 p 的倍数. 则

$$\left|\sum_{x=1}^{p^{l+t}} e_{p^l}(f(x))\right| \leqslant c_4(k)p^{l(1-a)}.$$

证　由于 $d|k!$, 所以得此推论.

推论 1.2　命 $f(x)$ 是一 k 次整值多项式, 它的系数的最小公分母是 d. 假定对 q 的任一素因子 p, 并非 $f(x)$ 的所有非常数项的系数的分子都是 p 的倍数. 则

$$\left|\sum_{x=1}^{\bar{q}} e_q(f(x))\right| \leqslant c_5(k, \varepsilon)q^{1-a+\varepsilon},$$

此处 $\bar{q} = q \cdot \prod_{\substack{p|q \\ p^t \| \sigma}} p^t$.

推论 1.3　仍如推论 1.1 及 1.2 的假定, 我们有

$$\left|\sum_{\substack{x=1 \\ p\nmid x}}^{p^{l+t}} e_{p^l}(f(x))\right| \leqslant c_6(k)p^{(1-a)l}$$

及

$$\left|\sum_{\substack{x=1 \\ (x,q)=1}}^{\bar{q}} e_q(f(x))\right| \leqslant c_7(k,\varepsilon)q^{1-a+\varepsilon}.$$

证　我们现在仅证明第一不等式, 第二式可由第一式推得. 显然有

$$\sum_{\substack{x=1 \\ p\nmid x}}^{p^{l+t}} e_{p^l}(f(x)) = \sum_{x=1}^{p^{l+t}} e_{p^l}(f(x)) - \sum_{x=1}^{p^{l+t-1}} e_{p^l}(f(px)).$$

写

$$df(x) = a_k x^k + \cdots + a_1 x + a_0, \quad p \nmid (a_k, \cdots a_1).$$

命 p^μ 是 p 的最高方次可以整除 $(f(px) - f(0))d$ 的所有的系数者. 显然 $1 \leqslant \mu \leqslant k$. 所以当 $l \geqslant \mu$ 时,

$$\begin{aligned}\left|\sum_{x=1}^{p^{l+t-1}} e_{p^l}(f(px))\right| &= \left|\sum_{x=1}^{p^{l+t-1}} e_{p^{l-\mu}}(p^{-\mu}(f(px) - f(0)))\right| \\ &\leqslant p^{\mu-1} \cdot c_4(k)p^{(l-\mu)(1-a)} \\ &\leqslant c_4(k)p^{l(1-a)-1+\mu a} \leqslant c_4(k)p^{l(1-a)}.\end{aligned}$$

若 $l < \mu \leqslant k$, 则显然有

$$\left|\sum_{x=1}^{p^{l+t-1}} e_{p^l}(f(px))\right| \leqslant p^{l+t-1} \leqslant k!p^{l-1} \leqslant k!p^{(1-a)l}.$$

§1.7　有限的傅里叶级数

引理 1.8　命

$$S = \sum_{q' < n \leqslant q''} e(n\,\alpha), \quad e(x) = \mathrm{e}^{2\pi i x},$$

则得

$$|S| \leqslant \min\left(q''-q', \frac{1}{2\{\alpha\}}\right),$$

此处 $\{\alpha\}$ 代表从 α 到和它最接近的整数的距离. 换言之, $\{\alpha\}=\min(\alpha-[\alpha],[\alpha]+1-\alpha)$.

证　显然有不等式 $|S|\leqslant q''-q'$. 若 $\alpha\neq[\alpha]$, 命 $Q=q''-q'$, 则有

$$\left|\sum_{q'<n\leqslant q''} e(n\,\alpha)\right| = \left|\sum_{n=0}^{Q-1} e(n\,\alpha)\right| = \left|\frac{1-e(Q\,\alpha)}{1-e(\alpha)}\right| \leqslant \frac{2}{|1-e(\alpha)|}$$
$$= \frac{1}{|\sin\pi\alpha|} \leqslant \frac{1}{2\{\alpha\}}.$$

$\left(当\ 0\leqslant\xi\leqslant\dfrac{1}{2}\ 时\ \sin\pi\xi>2\xi,\ 所以有\ |\sin\pi\xi|\geqslant 2\{\xi\}\right)$.

引理 1.9　命 $g(x)$ 表一周期是 q 的函数, 且

$$g(x)=\begin{cases}1, & 当\ 0<x\leqslant m,\\ 0, & 当\ m<x\leqslant q,\end{cases}$$

则

$$g(x)=\frac{m}{q}+\frac{1}{q}\sum_{n=1}^{q-1} e_q(n\,x)\sum_{t=1}^{m} e_q(-nt).$$

证　显然 $g(x)$ 可以表成

$$g(x)=\frac{1}{q}\sum_{n=1}^{q} e_q(n\,x)\sum_{t=1}^{m} e_q(-nt)$$
$$=\frac{m}{q}+\frac{1}{q}\sum_{n=1}^{q-1} e_q(n\,x)\sum_{t=1}^{m} e_q(-nt).$$

§1.8

定理 2　设 $f(x)=a_kx^k+\cdots+a_1x+a_0$ 是一整数系数多项式. 命 $(a_k,\cdots,a_2,q)=d$, 则

$$\left|\sum_{x=1}^{m} e_q(f(x))-\frac{m}{q}S(q,f(x))\right| \leqslant c_8(k,\varepsilon)q^{1-a+\varepsilon}d^{a}.$$

又当 $1\leqslant m\leqslant q$ 时

$$\left|\sum_{x=1}^{m} e_q(f(x))\right| \leqslant c_9(k,\varepsilon)q^{1-a+\varepsilon}d^{a}.$$

证　由引理 1.9 已知

$$\sum_{x=1}^{m} e_q(f(x)) = \sum_{x=1}^{q} e_q(f(x))g(x)$$
$$= \frac{m}{q}S(q, f(x)) + \frac{1}{q}\sum_{x=1}^{q} e_q(f(x))\sum_{n=1}^{q-1} e_q(nx)\sum_{t=1}^{m} e_q(-nt),$$

即得 (由引理 1.8)

$$\left|\sum_{x=1}^{m} e_q(f(x)) - \frac{m}{q}S(q, f(x))\right| \leqslant \frac{1}{q}\sum_{n=1}^{q-1}\frac{1}{2\left\{\dfrac{n}{q}\right\}}\left|\sum_{x=1}^{q} e_q(f(x)+nx)\right|.$$

命 $(d, a_1+n) = q'$, 则由定理 1 可知

$$\frac{1}{q}\sum_{n=1}^{q-1}\frac{1}{2\left\{\dfrac{n}{q}\right\}}\left|\sum_{x=1}^{q} e_q(f(x)+nx)\right|$$
$$\leqslant \frac{1}{q}\sum_{q'|d}\sum_{\substack{n=1\\ a_1+n\equiv 0 \pmod{q'}}}^{q-1}\frac{1}{2\left\{\dfrac{n}{q}\right\}}\left|\sum_{x=1}^{q} e_{q/q'}\left(\frac{f(x)+nx}{q'}\right)\right|$$
$$\ll \frac{1}{q}\sum_{q'|d}\sum_{\substack{n=1\\ a_1+n\equiv 0 \pmod{q'}}}^{q-1}\frac{1}{\left\{\dfrac{n}{q}\right\}}q'\left(\frac{q}{q'}\right)^{1-a+\epsilon}$$
$$\ll q^{1-a+\varepsilon}\left(\sum_{q'|d} q'^{a}\left(\sum_{\substack{1\leqslant n\leqslant q/2\\ a_1+n\equiv 0 \pmod{q'}}}\frac{1}{n} + \sum_{\substack{1\leqslant n\leqslant q/2\\ a_1-n\equiv 0 \pmod{q'}}}\frac{1}{n}\right)\right)$$
$$\ll q^{1-a+\varepsilon}\sum_{q'|d} q'a \ll q^{1-a+\epsilon}d^{a}.$$

第 2 章　包含除数函数的和的估值

§2.1　引　言

本章的目的在于证明以下的定理.

定理 3　命 $f(x_1, x_2, \cdots, x_n)$ 代表一个 k 次多项式, 它的系数是整数, 并假定所有的系数的最大公约数是 1, 则

$$\sum_{\substack{x_1=1 \\ f(x_1,\cdots,x_n)\neq 0}}^{P} \cdots \sum_{x_n=1}^{P} d^l(|f(x_1, \cdots, x_n)|) \leqslant c_1(k, n, l) A (\log X)^{c_2(k,n,l)},$$

此处 X 表 $|f(x_1, \cdots, x_n)|$ 在 $1 \leqslant x_1, \cdots, x_n \leqslant P$ 中的最大值, $A = \max(P^n, X^{n/k})$.

注意, 此处 c_1 及 c_2 与 $f(x_1, \cdots, x_n)$ 的系数并无关系. 由此定理容易引出下面较广泛的推理:

命 $f(x_1, \cdots, x_n)$ 代表一个 k 次整系数多项式. 命 m 代表它的所有的系数的最大公约数, 则

$$\sum_{\substack{x_1=1 \\ f(x_1,\cdots,x_n)\neq 0}}^{P} \cdots \sum_{x_n=1}^{P} d^l(|f(x_1, \cdots, x_n)|) \leqslant c_1(k, n, l) A (\log X)^{c_2(k,n,l)} d^l(m).$$

定理 3 的证明依赖于 van der Corput 的一个引理 (§2) 和第 1 章所证明的关于三角和的结果.

§2.2　van der Corput 的引理 *

引理 2.1　设有正数 A 及 γ 存在, 使

$$\sum_{\substack{y=1 \\ v|y}}^{X} T(y) \leqslant A \prod_{\sigma=1}^{s} \frac{x(p_\sigma, \alpha_\sigma)}{p_\sigma}, \quad v = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \leqslant X^\gamma,$$

此处 $T(y) \geqslant 0, x(p_\sigma, \alpha_\sigma) \geqslant 0$; 且

$$\sum_{\alpha=1}^{\infty} (\alpha+1)^{(1+2/\gamma)l} x(p, \alpha) \leqslant C,$$

---

* *Proc, Akad. Wetensch. Amsterdam*, 42(1939).

此处 C 与素数 p 无关. 又当 $v=1, s=0$ 时, 有不等式

$$\sum_{y=1}^{X} T(y) \leqslant A,$$

则

$$S=\sum_{y=1}^{X} d^{l}(y) T(y) \leqslant c_{3}(l, C, \gamma) A(\log X)^{c}.$$

证　把 y 写成 $y=P_{1} P_{2} \cdots P_{m} w$, 此处 P 经过 y 的所有大于 X^{γ} 的素数因子. 以 v_{1} 表 w 的不大于 X^{γ} 之最大因子, v_{2} 表 w / v_{1} 的不大于 X^{γ} 之最大因子, 依此进行. 假定此手续止于 n 次, 则 y 可以表成

$$y=P_{1} \cdots P_{m} v_{1} \cdots v_{n} .$$

这 n 将称为 y 的指标, 而 $v_{1}, \cdots, v_{n}$ 将称为 y 的特征因数.

显然有 $v_{n-1} \geqslant X^{\frac{1}{2} \gamma}$, 由此得

$$X^{\gamma m} \leqslant P_{1} \cdots P_{m} \leqslant X, \quad X^{\frac{1}{2}(n-1) \gamma} \leqslant v_{1} \cdots v_{n-1} \leqslant X,$$

即得

$$m \leqslant \frac{1}{\gamma}, \quad n \leqslant 1+\frac{2}{\gamma} .$$

由 $d(\lambda \mu) \leqslant d(\lambda) d(\mu)$, 可知

$$d(y) \leqslant 2^{m} d(v_{1}) \cdots d(v_{n}) \leqslant 2^{1 / \gamma} d(v_{1}) \cdots d(v_{n}) .$$

显然有

$$d^{l}(y) \leqslant \begin{cases}2^{l / \gamma}, & \text{若 } n=0, \\ 2^{l / \gamma} \max\limits_{v} d^{l n}(v_{v}) \leqslant 2^{l / \gamma} \sum\limits_{v=1}^{n} d^{l n}(v_{v}), & \text{若 } n>0 .\end{cases}$$

写

$$S=\sum_{y=1}^{X} d^{l}(y) T(y)=\sum_{0 \leqslant n \leqslant 1+2 / \gamma} U_{n},$$

分和 U_{n} 代表 S 中所有 y 的指标是 n 的项之和.

当 $n=0$ 时,

$$U_{0} \leqslant 2^{l / \gamma} \sum_{y=1}^{X} T(y) \leqslant 2^{l / \gamma} A .$$

若 $1 \leqslant n \leqslant 1+\dfrac{2}{\gamma}$, 则

$$U_{n} \leqslant 2^{l / \gamma} \sum_{v=1}^{n} U_{n v},$$

其中

$$U_{nv}=\sum_{y=1}^{X}{}'d^{ln}(v_v)T(y),$$

此处 $\sum\limits_{y=1}^{X}{}'$ 表示一个和, 其中 y 经过一切指标是 n 的数, 且以 v_v 做它的第 v 个特征因子者. 已知 $2\leqslant v_v\leqslant X^{\gamma}$, 所以

$$U_{nv}\leqslant\sum_{2\leqslant v\leqslant X^{\gamma}}d^{ln}(v)\sum_{y=1}^{X}{}''T(y),$$

此处 $\sum\limits_{y=1}^{X}{}''$ 表示一个和, 其中 y 的指标是 n 且以 v 做它的第 v 个特征因子者. 因此

$$\sum_{y=1}^{X}{}''T(y)\leqslant\sum_{\substack{y=1\\ i|y}}^{X}T(y)\leqslant A\prod_{\sigma=1}^{s}\frac{x(p_\sigma,\alpha_\sigma)}{p_\sigma}.$$

由于 $d(v)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1)$, 可知

$$\begin{aligned}U_{nv}&\leqslant A\sum_{2\leqslant v\leqslant X^{\gamma}}\prod_{\sigma=1}^{s}\frac{(\alpha_\sigma+1)^{ln}x(p_\sigma,\alpha_\sigma)}{p_\sigma}\\&\leqslant A\prod_{p\leqslant X^{\gamma}}\left(1+\sum_{\alpha=1}^{\infty}\frac{(\alpha+1)^{ln}x(p,\alpha)}{p}\right)\\&\leqslant Ae^{R}\leqslant c_3'Ae^{c\log\log X}\leqslant c_3'A(\log X)^{c},\end{aligned}$$

此处 $R=c\sum\limits_{p\leqslant x^{\gamma}}\frac{1}{p}$. 代入关于 U_n 及 S 的不等式, 由此即得出本引理.

(注意, 在证明中用了等式

$$\sum_{p\leqslant X}\frac{1}{p}=\log\log X+O(1).$$

这是素数定理的推理. 当然也是引理 7.14 的推理.)

§2.3　关于相合式解数的若干引理

引理 2.2　命 $f(x_1,\cdots,x_n)$ 是具有整数系数的 k 次多项式. 并且假定并非它所有的系数都是 p 的倍数. 则相合式

$$f(x_1,\cdots,x_n)\equiv 0\pmod{p^{\alpha}}$$

的解数 $\leqslant c_4(k,n)p^{n\alpha-1}$.

证 1) 当 $n=1$, 这引理显然正确, 因为相合式

$$f(x)\equiv 0 \pmod p$$

的根数不超过 k, 所以原相合式的解数 $\leqslant kp^{\alpha-1}$.

2) 将相合式 $f(x_1,\cdots,x_n)\equiv 0 \pmod{p^\alpha}$ 写成

$$f_s(x_1,\cdots,x_{n-1})x_n^s+\cdots+f_0(x_1,\cdots,x_{n-1})\equiv 0 \pmod{p^\alpha}.$$

我们现用归纳法来证明本引理. 假定本引理对 $n-1$ 个变数是真实的, 则

$$f_s(x_1,\cdots,x_{n-1})\equiv 0 \pmod{p^\alpha}$$

的解数是 $O(p^{(n-1)\alpha-1})$. 如果 $f_s(x_1,\cdots,x_{n-1})\not\equiv 0 \pmod{p^\alpha}$, 则原式中 x_n 之值最多是 $O(p^{\alpha-1})$. 所以所讨论的相合式的解数 $\leqslant c_4(k,n)p^{n\alpha-1}$.

引理 2.3 在引理 2.2 的假设下, 相合式

$$f(x_1,\cdots,x_n)\equiv 0 \pmod{p^\alpha}$$

的解数 $\leqslant c_5(k,n)(\alpha+1)^{n-1}p^{n\alpha-\alpha a}$, 此处 $a=1/k$.

证 1) 当 $n=1$, 相合式

$$f(x)\equiv 0 \pmod{p^\alpha}$$

的解数等于

$$\frac{1}{p^\alpha}\sum_{h=1}^{p^\alpha}\sum_{x=1}^{p^\alpha}e_{p^\alpha}(hf(x)),\quad e_q(x)=\mathrm{e}^{2\pi\mathrm{i}x/q}.$$

命

$$f(x)=a_kx^k+\cdots+a_1x+a_0.$$

若 $p|(a_k,\cdots,a_1)$ 而 $p\nmid a_0$, 则此相合式无解, 引理显然成立. 今假定 $p\nmid(a_k,\cdots,a_1)$. 由引理 1.1,

$$\begin{aligned}\left|\frac{1}{p^\alpha}\sum_{h=1}^{p^\alpha}\sum_{x=1}^{p^\alpha}e_{p^\alpha}(hf(x))\right| &\leqslant \frac{1}{p^\alpha}\sum_{h=1}^{p^\alpha}\left|\sum_{x=1}^{p^\alpha}e_{p^\alpha}(hf(x))\right|\\ &=\frac{1}{p^\alpha}\sum_{\lambda=0}^{\alpha}\sum_{\substack{h=1\\p^\lambda\|h}}^{p^\alpha}\left|\sum_{x=1}^{p^\alpha}e_{p^\alpha}(hf(x))\right|\end{aligned}$$

$$= O\left(\frac{1}{p^\alpha}\sum_{\lambda=0}^{\alpha} p^{\alpha-\lambda}\cdot p^\lambda \cdot p^{(\alpha-\lambda)(1-a)}\right)$$
$$= O(p^{\alpha(1-a)}),$$

此处用上了

$$\sum_{\lambda=0}^{\alpha} p^{-\lambda(1-a)} = O(1).$$

2) 归纳法. 把式子

$$f(x_1,\cdots,x_n)\equiv 0 \pmod{p^\alpha}$$

写成

$$g_k x_n^k+\cdots+g_0\equiv 0 \pmod{p^\alpha},\quad g_v=g_v(x_1,\cdots,x_{n-1}).$$

今分别讨论使

$$p^\lambda \| (g_k,\cdots,g_0),\quad \alpha>\lambda>0, \tag{1}$$

以及使 $p^\alpha|(g_k,\cdots,g_0)$ 的整数组 $x_1,\cdots,x_{n-1}$. 在后一种情况之下, 其解数是

$$O((\alpha+1)^{n-2}p^{(n-1)\alpha-\alpha a}p^\alpha)=O((\alpha+1)^{n-2}p^{n\alpha-\alpha a}).$$

今讨论具有条件 (1) 的情况. 在所有的 g 之中, 至少有一个并非所有的系数都是 p 的倍数的, 以 g_μ 表之. 由归纳法假定, 适合

$$g_\mu\equiv 0 \pmod{p^\lambda},\quad 0\leqslant x_v<p^\alpha,\quad 1\leqslant v\leqslant n-1$$

的解数最多是

$$O((\alpha+1)^{n-2}p^{(n-1)(\alpha-\lambda)+(n-1)\lambda-\lambda\alpha})=O((\alpha+1)^{n-2}p^{(n-1)\alpha-\lambda\alpha}),$$

即适合条件 (1) 的 $x_1,\cdots,x_{n-1}$ 的组数是 $O((\alpha+1)^{n-2}p^{(n-1)\alpha-\lambda a})$. 对每一组适合 (1) 的 $x_1,\cdots,x_{n-1}$, 相合式

$$\frac{g_k}{p^\lambda}x_n^k+\cdots+\frac{g_0}{p^\lambda}\equiv 0 \pmod{p^{\alpha-\lambda}},\quad 0<x_n\leqslant p^\alpha,$$

最多有 $O(p^{\lambda+(\alpha-\lambda)(1-a)})=O(p^{\alpha-(\alpha-\lambda)a})$ 个 x_n.

所以引理中所涉及的适合 (1) 的相合式的解是

$$O((\alpha+1)^{n-2}p^{(n-1)\alpha-\lambda a}p^{\alpha-(\alpha-\lambda)a})=O((\alpha+1)^{n-2}p^{n\alpha-a\alpha}).$$

$\lambda=0$ 时此结论也显然真实. 所以引理中相合式的解数是

$$O\left(\sum_{\lambda=0}^{\alpha}(\alpha+1)^{n-2}p^{n\alpha-a\alpha}\right)=O((\alpha+1)^{n-1}p^{n\alpha-a\alpha}).$$

§2.4　定理的证明

在引理 2.1 中取 $T(y)$ 为

$$|f(x_1,\cdots,x_n)|=y,\quad 1\leqslant x_v\leqslant P$$

的解数. 则得

$$\sum_{\substack{x_1=1\\ f(x_1,\cdots,x_n)\neq 0}}^{P}\cdots\sum_{x_n=1}^{P}d^l(|f(x_1,\cdots,x_n)|)=\sum_{y=1}^{X}d^l(y)T(y),$$

此处 X 是 $|f(x_1,\cdots,x_n)|$ 在 $1\leqslant x_1,\cdots,x_n\leqslant P$ 中的极大值.

取 $\gamma=a$ 及

$$x(p,\alpha)=\begin{cases}O(1), & 当\ \alpha\leqslant k,\\ O((\alpha+1)^{n-1}p^{1-a\alpha}), & 当\ \alpha>k,\end{cases}$$

则

$$\sum_{y=1}^{X}T(y)=\sum_{x_1=1}^{P}\cdots\sum_{x_n=1}^{P}1=P^n\leqslant A.$$

又

$$\sum_{\substack{y=1\\ v|y}}^{X}T(y)\leqslant\left(\frac{P}{v}+1\right)^n M,$$

此处 M 是

$$f(x_1,\cdots,x_n)\equiv 0\pmod v$$

的解数. 但此相合式之解数为诸相合式

$$f(x_1,\cdots,x_n)\equiv 0\pmod{p_\sigma^{\alpha_\sigma}},\quad \sigma=1,\cdots,s$$

的解数之积, 故由引理 2.2 及 2.3 可知

$$\sum_{\substack{y=1 \\ v|y}}^{X} T(y) = O\left(\left(\frac{p}{v}+1\right)^n \prod_{\sigma=1}^{s} p_\sigma^{n\alpha_\sigma} \frac{x(p_\sigma,\alpha_\sigma)}{p_\sigma}\right)$$

$$= O\left(A \prod_{\sigma=1}^{s} \frac{x(p_\sigma,\alpha_\sigma)}{p_\sigma}\right).$$

由于

$$\sum_{\alpha=1}^{\infty} (\alpha+1)^{(1+2/\gamma)l} x(p,\alpha) = O\Bigg(\sum_{a\leqslant k}(\alpha+1)^{(1+2k)l} + \sum_{\alpha>k}(\alpha+1)^{(1+2k)l+n-1}p^{1-a\alpha}\Bigg) = O(1),$$

所以证明了我们的定理.

§2.5

为了将来的应用, 我们证明两条较精密且特殊的结果, 这些结果也是和除数函数和有关的.

引理 2.4　命 t 是一正整数, 则

$$\sum_{0<z\leqslant P} \frac{(d(z))^t}{z} \leqslant c_6(t)\ (\log\ P)^{2^t}.$$

证　当 $t=0$ 时上式显然正确. 今设其对 $t-1$ 也真. 则

$$\sum_{0<z\leqslant P} \frac{(d(z))^t}{z} = \sum_{0<z\leqslant P} \frac{(d(z))^{t-1}}{z} \sum_{\lambda|z} 1 = \sum_{0<\lambda\leqslant P} \sum_{\substack{0<z\leqslant P \\ \lambda|z}} \frac{(d(z))^{t-1}}{z}$$

$$\leqslant \sum_{0<\lambda\leqslant P} \frac{(d(\lambda))^{t-1}}{\lambda} \sum_{0<\mu\leqslant P/\lambda} \frac{(d(\mu))^{t-1}}{\mu} \leqslant (c_6(t-1))^2 (\log\ P)^{2^t}.$$

引理 2.5　命 t 是一正整数, 则

$$\sum_{0<z\leqslant P} (d(z))^t \leqslant c_7(t) P (\log\ P)^{2^t-1}.$$

证　由引理 2.4 及归纳法可知

$$\begin{aligned}
\sum_{0<z\leqslant P}(d(z))^t &= \sum_{0<z\leqslant P}(d(z))^{t-1}\sum_{\lambda|z}1 = \sum_{0<\lambda\leqslant P}\sum_{\substack{0<z\leqslant P\\ \lambda|z}}(d(z))^{t-1}\\
&\leqslant \sum_{0<\lambda\leqslant P}(d(\lambda))^{t-1}\sum_{0<\mu\leqslant P/\lambda}(d(\mu))^{t-1}\\
&= O\left(\sum_{0<\lambda\leqslant P}(d(\lambda))^{t-1}\frac{P}{\lambda}(\log P)^{2^{t-1}-1}\right) = O\left(P(\log P)^{2^t-1}\right).
\end{aligned}$$

第 3 章　某些三角和的中值定理 (I)

§3.1

定理 4　命 $f(x)$ 代表一个 k 次整值多项式,

$$T(\alpha)=\sum_{x=1}^{P}e(f(x)\alpha),$$

则当 $1\leqslant v\leqslant k$ 时, 我们有

$$\int_0^1|T(\alpha)|^{2v}\mathrm{d}\alpha\leqslant c_1(k,v)P^{2^v-v}(\log P)^{c_2(k,v)}d^{v-1}(u),$$

此处 u 是 $f(x)$ 的系数的分子之最大公约数, $c(k,v)$ 仅依于 k 及 v 而与 $f(x)$ 的系数无关.

附记: 因为

$$g(\lambda)=\log\left(\int_0^1|T(\alpha)|^{\lambda}\mathrm{d}\alpha\right)$$

是一凸函数, 所以我们可以得出关于任一实数 λ 的不等式. 确切些说: 当 $2^v<\lambda\leqslant 2^{v+1}$ 时有不等式

$$\int_0^1|T(\alpha)|^{\lambda}\mathrm{d}\alpha\leqslant\left(\int_0^1|T(\alpha)|^{2^v}\mathrm{d}\alpha\right)^{2-2^{-v}\lambda}\left(\int_0^1|T(\alpha)|^{2^{v+1}}\mathrm{d}\alpha\right)^{2^{-v}\lambda-1}.$$

因为本文中以后不引用这一结果, 所以我们不证明这一结果.

§3.2　关于不等式的若干引理

引理 3.1　若 $\alpha+\beta=1,\alpha>0,\beta>0,s\geqslant 0,t\geqslant 0$, 则

$$s^{\alpha}t^{\beta}\leqslant s\alpha+t\beta. \tag{1}$$

一般地, 若 $\alpha_1+\cdots+\alpha_n=1,\alpha_1>0,\cdots,\alpha_n>0,s_1\geqslant 0,\cdots,s_n\geqslant 0$, 则

$$s_1^{\alpha_1}\cdots s_n^{\alpha_n}\leqslant s_1\alpha_1+\cdots+s_n\alpha_n. \tag{2}$$

证 1) 当 $x>1, 0<m<1$; 我们有

$$x^m-1=m\int_1^x y^{m-1}\mathrm{d}y\leqslant m\int_1^x \mathrm{d}y=m(x-1).$$

取 $x=\frac{s}{t}(s>t), m=\alpha$ 及 $1-m=\beta$, 即得 (1) 式.

2) 由 (1) 式知当 $n=2$ 时 (2) 式成立. 今用归纳法. 设 (2) 式当 $n-1$ 时已成立, 于是

$$\begin{aligned}s_1^{\alpha_1}\cdots s_n^{\alpha_n}=&\left(s_1^{\frac{\alpha_1}{1-\alpha_n}}\cdots s_{n-1}^{\frac{\alpha_{n-1}}{1-\alpha_n}}\right)^{1-\alpha_n}s_n^{\alpha_n}\leqslant\left(s_1^{\frac{\alpha_1}{1-\alpha_n}}\cdots s_{n-1}^{\frac{\alpha_{n-1}}{1-\alpha_n}}\right)(1-\alpha_n)\\&+s_n\alpha_n\leqslant\left(s_1\frac{\alpha_1}{1-\alpha_n}+\cdots+s_{n-1}\frac{\alpha_{n-1}}{1-\alpha_n}\right)(1-\alpha_n)+s_n\alpha_n\\=&s_1\alpha_1+\cdots+s_{n-1}\alpha_{n-1}+s_n\alpha_n.\end{aligned}$$

此即 (2) 式.

引理 3.2 若 $\alpha+\beta=1, \alpha>0, \beta>0$, 则对实数 a_n 及 $b_n(1\leqslant n\leqslant r)$ 常有

$$\left|\sum_{n=1}^r a_nb_n\right|\leqslant\left(\sum_{n=1}^r|a_n|^{\frac{1}{\alpha}}\right)^\alpha\left(\sum_{n=1}^r|b_n|^{\frac{1}{\beta}}\right)^\beta$$

(以后引证时, 这不等式将称为 Hölder 不等式. 而 $\alpha=\beta=\frac{1}{2}$ 的特例, 将称为Буняковский, Cauchy 或 Schwarz 不等式).

证 由引理 3.1 可知

$$\begin{aligned}\frac{\sum\limits_{n=1}^r|a_nb_n|}{\left(\sum\limits_{n=1}^r|a_n|^{\frac{1}{\alpha}}|\right)^\alpha\left(\sum\limits_{n=1}^r|b_n|^{\frac{1}{\beta}}\right)^\beta}&=\sum_{n=1}^r\left(\frac{|a_n|^{\frac{1}{\alpha}}}{\sum\limits_{n=1}^r|a_n|^{\frac{1}{\alpha}}}\right)^\alpha\left(\frac{|b_n|^{\frac{1}{\beta}}}{\sum\limits_{n=1}^r|b_n|^{\frac{1}{\beta}}}\right)^\beta\\&\leqslant\sum_{n=1}^r\left(\frac{\alpha|a_n|^{\frac{1}{\alpha}}}{\sum\limits_{n=1}^r|a_n|^{\frac{1}{\alpha}}}+\frac{\beta|b_n|^{\frac{1}{\beta}}}{\sum\limits_{n=1}^r|b_n|^{\frac{1}{\beta}}}\right)=\alpha+\beta=1.\end{aligned}$$

引理 3.3 命

$$\mathop{\Delta}_{y}Q(x)=\frac{1}{y}(Q(x+y)-Q(x)),\quad I=\sum_{x=1}^P e(f(x)).$$

今用符号 $\sum\limits_x^P$ 表示一和*, 此和可以分为 $c_2(k)$ 段, 每段的求和变数 x 过 $\leqslant P$ 个连

* 此符号以后将经常采用.

续整数. 则当 $\mu=1,2,\cdots,k$ 时有次之不等式

$$|I|^{2^\mu}\leqslant c_3(\mu)P^{2^\mu-\mu-1}\sum_{y_1}^{P}\cdots\sum_{y_\mu}^{P}\sum_{x_{\mu+1}}^{P}e(y_1\cdots y_\mu\underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta}f(x_{\mu+1})).$$

证　由等式

$$\begin{aligned}|I|^2&=\sum_{x_1=1}^{P}\sum_{x_2=1}^{P}e(f(x_1)-f(x_2))\\&=\sum_{x_2}^{P}\sum_{y_1}^{P}e(f(x_2+y_1)-f(x_2))\\&=\sum_{y_1}^{P}\sum_{x_2}^{P}e(y_1\underset{y_1}{\Delta}f(x_2)),\end{aligned}$$

可知引理当 $\mu=1$ 时为真.

今假定本引理对 $\mu-1$ 为真. 用 Cauchy 不等式得出

$$\begin{aligned}&|I|^{2^\mu}=(|I|^{2^{\mu-1}})^2\\&\leqslant(c_3(\mu-1))^2P^{2(2^{\mu-1}-\mu)}\left|\sum_{y_1}^{P}\cdots\sum_{y_{\mu-1}}^{P}\sum_{x_\mu}^{P}e(y_1\cdots y_{\mu-1}\underset{y_{\mu-1}}{\Delta}\cdots\underset{y_1}{\Delta}f(x_\mu))\right|^2\\&\ll P^{2^\mu-2\mu}P^{\mu-1}\sum_{y_1}^{P}\cdots\sum_{y_{\mu-1}}^{P}\left|\sum_{x_\mu}^{P}e(y_1\cdots y_{\mu-1}\underset{y_{\mu-1}}{\Delta}\cdots\underset{y_1}{\Delta}f(x_\mu))\right|^2\\&\ll P^{2^\mu-\mu-1}\sum_{y_1}^{P}\cdots\sum_{y_\mu}^{P}\sum_{x_{\mu+1}}^{P}e(y_1\cdots y_\mu\underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta}f(x_{\mu+1})).\end{aligned}$$

引理 3.4　若 $Q(x)$ 是一 k 次多项式, 其最高方次的系数是 α, 则 $\underset{y}{\Delta}Q(x)$ 是 x 的 $(k-1)$ 次多项式, 其最高方次的系数是 $k\alpha$. 由此推得

$$\begin{aligned}\underset{y_1}{\Delta}\cdots\underset{y_{k-1}}{\Delta}Q(x)&=k!\alpha x+\beta,\\\underset{y_1}{\Delta}\cdots\underset{y_k}{\Delta}Q(x)&=k!\alpha.\end{aligned}$$

此引理的证明十分明显.

§3.3　定理的证明

并不失去普遍性, 我们可假定 $f(x)$ 是整系数多项式. 因为如果 q 是 $f(x)$ 的系

数的最小公分母, 则由 Hölder 不等式 (引理 3.2) 可得

$$\int_0^1 |T(\alpha)|^\lambda \mathrm{d}\alpha = \int_0^1 \left|\sum_{t=1}^{q}\sum_{x=0}^{[(P-t/q)]} e(f(qx+t)\alpha)\right|^\lambda \mathrm{d}\alpha$$

$$\leqslant q^{\lambda-1}\sum_{t=1}^{q}\int_0^1 \left|\sum_{x=0}^{[(P-t)/q]} e((f(qx+t)-f(t))\alpha)\right|^\lambda \mathrm{d}\alpha,$$

此处 $f(qx+t)-f(t)$ 是整系数多项式. 又注意 $q \leqslant k!$.

当 $v=1$ 时此定理显然真实. 由引理 3.3 得出

$$|T(\alpha)|^{2^\mu} \ll P^{2^\mu-1} + P^{2^\mu-\mu-1}\sum_{y_1}^{P}\cdots\sum_{y_\mu}^{P}\sum_{x_{\mu+1}}^{P}{}^{*} e(y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1})\alpha), \tag{1}$$

此处星号 $*$ 代表条件

$$y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1}) \neq 0.$$

其中用到由 $y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1})=0$ 可知有一个 v 使 $y_v=0$ 或 $\underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1})=0$. 因为 $\underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1})$ 的最高系数非零, 所以得出 (1) 式.

以 $|T(\alpha)|^{2^\mu}$ 乘不等式双方, 并且对 α 由 0 至 1 求积分, 即得

$$\left.\begin{aligned}&\int_0^1 |T(\alpha)|^{2^{\mu+1}}\mathrm{d}\alpha \ll P^{2^\mu-1}\int_0^1 |T(\alpha)|^{2^\mu}\mathrm{d}\alpha\\ &+P^{2^\mu-\mu-1}\int_0^1\sum_{y_1}^{P}\cdots\sum_{y_\mu}^{P}\sum_{x_{\mu+1}}^{P}{}^{*} e(y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1})\alpha)|T(\alpha)|^{2^\mu}\mathrm{d}\alpha.\end{aligned}\right\} \tag{2}$$

由归纳法假定可知 (2) 式右边的第一项是

$$\begin{aligned}&O(P^{2^\mu-1}P^{2^\mu-\mu}(\log P)^{c_2(k,\mu)}(d(u))^{\mu-1})\\ =&O(P^{2^{\mu+1}-\mu-1}(\log P)^{c_2(k,\mu)}(d(u))^{\mu-1}).\end{aligned}$$

(2) 式右边的第二项等于

$$\begin{aligned}&P^{2^\mu-\mu-1}\int_0^1\sum_{y_1}^{P}\cdots\sum_{y_\mu}^{P}\sum_{x_{\mu+1}}^{P}{}^{*}\sum_{z_1}^{P}\sum_{z_{2^\mu}}^{P} e((y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1})\\ &-f(z_1)-\cdots-f(z_{2^{\mu-1}})+f(z_{2^{\mu-1}+1})+\cdots+f(z_{2^\mu}))\alpha)d\alpha\\ =&P^{2^\mu-\mu-1}R,\end{aligned}$$

此处 R 是下列方程式的整数解的组数:

$$\left.\begin{array}{r} y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1}) = f(z_1)+\cdots+f(z_{2^{\mu-1}})-f(z_{2^{\mu-1}+1})-\cdots-f(z_{2^\mu}), \\ y_1\cdots y_\mu \underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta} f(x_{\mu+1}) \neq 0, \quad z_v, y_v, x_{v+1} \ll P. \end{array}\right\} \tag{3}$$

对已与的 $z_1,\cdots z_{2^\mu}$, (3) 式的解数

$$\ll d^\mu(f(z_1)+\cdots+f(z_{2^{\mu-1}})-f(z_{2^{\mu-1}+1})-\cdots-f(z_{2^\mu})).$$

由定理 3, 可知

$$\begin{aligned} R &\ll \sum_{z_1}^{P}\cdots\sum_{z_{2^\mu}}^{P}{}^{**} d^\mu(f(z_1)+\cdots-f(z_{2^\mu})) \\ &\ll d^\mu(u)P^{2^\mu}(\log P)^{c_2(k,\mu)}, \end{aligned}$$

此处 ** 号表示条件 $f(z_1)+\cdots-f(z_{2^\mu})\neq 0$. 定理已经证明.

§3.4　Weyl 的引理

引理 3.5　命 $q>0$,

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\quad (h,q)=1$$

及

$$Q=\sum_{x=f+1}^{f+q}\min\left(U,\frac{1}{2\{\alpha x\}}\right).$$

则

$$Q<6U+q\log q.$$

证　写成 $\alpha=\dfrac{h}{q}+\dfrac{\theta}{q^2}, |\theta|\leqslant 1$. 命 $x=x_1+f$; 则 $1\leqslant x_1\leqslant q$. 把 αf 写成

$$\alpha f=\frac{b}{q}+\frac{\theta'}{q},\quad |\theta'|\leqslant 1,\quad b: \text{整数}$$

的形式.

由于 $x_1\leqslant q$ 可得

$$\{\alpha x\}=\{\alpha x_1+\alpha f\}=\left\{\frac{hx_1}{q}+\frac{\theta x_1}{q^2}+\frac{b}{q}+\frac{\theta'}{q}\right\}=\left\{\frac{\rho+2\theta''}{q}\right\},\quad |\theta''|\leqslant 1,$$

此处 ρ 表示以 q 除 hx_1+b 所得的绝对值最小的剩余.

由于 $(h,q)=1$, 当 x_1 经过一完整的剩余系, mod q 时, ρ 经过 $0,1,\cdots,\left[\frac{1}{2}q\right]$, 并且同一 ρ 的值出现最多两次.

Q 中适合于 $\rho\leqslant 2$ 的各项用 U 代替它们, 其他诸项可以表成

$$\rho=2+s,\quad v<s\leqslant\frac{1}{2}q-2$$

的形式. 因此

$$\left\{\frac{\rho+2\theta''}{q}\right\}>\frac{s}{q}.$$

故知

$$Q\leqslant 6U+2\sum_{s=1}^{\left[\frac{1}{2}q-2\right]}\frac{1}{\frac{2s}{q}}<6U+q\log q.$$

引理 3.6(Weyl)　若 $\alpha_k,\cdots,\alpha_0$ 是实数,

$$f(x)=\alpha_kx^k+\cdots+\alpha_1x+\alpha_0,$$
$$\left|\alpha_k-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\quad (h,q)=1,$$

则

$$S=\sum_{x=1}^{P}e(f(x))\ll P^{1+\varepsilon}q^{\varepsilon}\left(\frac{1}{P}+\frac{1}{q}+\frac{q}{P^k}\right)^{2^{1-k}}.$$

证　由引理 3.3 及 3.4, 可得

$$\begin{aligned}|S|^{2^{k-1}}&\ll P^{2^{k-1}-k}\sum_{y_1}^{P}\cdots\sum_{y_{k-1}}^{P}\sum_{x_k}^{P}e(y_1\cdots y_{k-1}\mathop{\Delta}_{y_{k-1}}\cdots\mathop{\Delta}_{y_1}f(x_k))\\&\ll P^{2^{k-1}-k}\sum_{y_1}^{P}\cdots\sum_{y_{k-1}}^{P}\left|\sum_{x_k}^{P}e(k!y_1\cdots y_{k-1}x_k\alpha_k)\right|\\&\ll P^{2^{k-1}-1}+P^{2^{k-1}-k}\sum_{y_1}^{P}\cdots\sum_{y_{k-1}}^{P}{}^{*}\left|\sum_{x_k}^{P}e(k!y_1\cdots y_{k-1}x_k\alpha_k)\right|,\end{aligned}$$

此处 $*$ 表示条件 $y_1\cdots y_{k-1}\neq 0$. 由引理 1.2 已知

$$k!y_1\cdots y_{k-1}=Y,\quad Y\ll P^{k-1}$$

的解数 $\leqslant(d(Y))^{k-1}=O(P^{\varepsilon})$, 所以

$$|S|^{2^{k-1}}\ll P^{2^{k-1}-1}+P^{2^{k-1}-k+\varepsilon}\sum_{Y}^{P^{k-1}}\left|\sum_{x}^{P}e(Yx\alpha_k)\right|.$$

由引理 1.8 可知

$$\sum_{x}^{P} e(Yx\alpha_k) \ll \min\left(P, \frac{1}{\{Y\alpha_k\}}\right).$$

又由引理 3.5 可得

$$\begin{aligned}\sum_{Y}^{P^{k-1}} \min\left(P, \frac{1}{\{Y\alpha_k\}}\right) &\ll \left(\frac{P^{k-1}}{q}+1\right)\max_{f}\left(\sum_{Y=f+1}^{f+q}\min\left(P, \frac{1}{\{Y\alpha_k\}}\right)\right)\\ &\ll \left(\frac{P^{k-1}}{q}+1\right)(P+q\log q).\end{aligned}$$

由此得出

$$\begin{aligned}|S|^{2^{k-1}} &\ll P^{2^{k-1}-1} + P^{2^{k-1}-k+\varepsilon}\left(\frac{P^{k-1}}{q}+1\right)(P+q\log q)\\ &\ll P^{\varepsilon}q^{\varepsilon}P^{2^{k-1}}\left(\frac{1}{P}+\frac{1}{q}+\frac{q}{P^k}\right).\end{aligned}$$

第4章　Виноградов 的中值定理及其推论

§4.1　定理的叙述

在本章中我们将讨论最有名的Виноградов定理及其推论. 这一定理是解析数论新研究的一个基本工具.

定理 5(Виноградов的中值定理).　命

$$f(x)=\alpha_k x^k+\cdots+\alpha_1 x$$

及

$$C_k=C_k(P)=\sum_{x=1}^{P}e(f(x)).$$

命

$$t_1(k)=t_1=\begin{cases}\frac{1}{4}k(k+1)+lk, & \text{当 } k\equiv 0,3 \pmod 4,\\ \frac{1}{4}(k^2+k+2)+lk, & \text{当 } k\equiv 1,2 \pmod 4,\end{cases}$$

则当 $0\leqslant l\leqslant c_1(k)$ 时,

$$\int_0^1\cdots\int_0^1|C_k|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\leqslant c_2(k)P^{2t_1-\frac{1}{2}k(k+1)+\delta+\varepsilon},$$

此处

$$\delta=\delta(k)=\frac{1}{2}k(k+1)(1-a)^l,\quad a=1/k.$$

此定理可以叙述成另一种形式:

上积分的值显然等于方程组

$$x_1^h+\cdots+x_{t_1}^h=y_1^h+\cdots+y_{t_1}^h,\quad 1\leqslant h\leqslant k,$$
$$1\leqslant x_i,y_i\leqslant P$$

的解答 $x_1,\cdots,x_{t_1};y_1,\cdots,y_{t_1}$ 的组数. 今往证明, 对任一整数 T, 该积分也等于下列方程组

$$x_1^h+\cdots+x_{t_1}^h=y_1^h+\cdots+y_{t_1}^h,\quad 1\leqslant h\leqslant k,$$
$$T<x_i,y_i\leqslant T+P$$

的解答的组数. 命 $X_i = x_i - T, Y_i = y_i - T$, 则得

$$\sum_{i=1}^{t_1}(X_i+T)^h = \sum_{i=1}^{t_1}(Y_i+T)^h, \quad 1 \leqslant h \leqslant k.$$

展开此 h 方, 易见此方程组与

$$\sum_{i=1}^{t_1} X_i^h = \sum_{i=1}^{t_1} Y_i^h, \quad 1 \leqslant h \leqslant k$$

完全相当.

又因为 $(0 \leqslant r \leqslant 2t_1)$

$$\begin{aligned}&\int_0^1 \cdots \int_0^1 C_k^r \bar{C}_k^{2t_1-r} \mathrm{e}^{2\pi\mathrm{i}(N_1\alpha_1+\cdots+N_k\alpha_k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k \\ \leqslant &\int_0^1 \cdots \int_0^1 |C_k|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k,\end{aligned}$$

故由此定理, 可知方程组

$$\sum_{v=1}^{r} x_v^h - \sum_{v=r+1}^{2t_1} y_v^h = N_h, \quad 1 \leqslant h \leqslant k,\ 1 \leqslant x,\ y \leqslant P$$

的整数解答数

$$\leqslant c_2(k)P^{2t_1-\frac{1}{2}k(k+1)+\delta+\varepsilon}.$$

此定理之证明依于引理 4.1. 著者对于证明作了某些简化及精密化工作.

§4.2　引　　理

引理 4.1　命 $Q = RH, R > 1, H > 1$ 及

$$1 \leqslant g_1 < g_2 < \cdots < g_k \leqslant H, \quad g_v - g_{v-1} > 1,$$

此处 $g_1, \cdots, g_k$ 是整数. 又命 x_v 在隔间

$$-\omega + (g_v - 1)R \leqslant x_v < -\omega + g_v R, \quad 0 \leqslant \omega \leqslant Q$$

中变化. 则整数组 $x_1, \cdots, x_k$ 中使

$$x_1^h + \cdots + x_k^h, \quad 1 \leqslant h \leqslant k,$$

各在长度 $\leqslant Q^{h-1}(1 \leqslant h \leqslant k)$ 的隔间中的组数

$$\leqslant 2^k(2kH)^{\frac{1}{2}k(k-1)}.$$

证 当 $k=1$ 此引理显然真实. 假定此引理对 $k-1$ 真实. 命 $x_1,\cdots,x_k$ 及 $y_1,\cdots,y_k$ 是适合引理的要求的二整数组. 命 $s_h=\sum_{v=1}^{k}x_v^h$ 及 $s_h'=\sum_{v=1}^{k}y_v^h$. 并以 σ_h 及 σ_h' 各表 $x_1,\cdots,x_k$ 及 $y_1,\cdots,y_k$ 的 h 次初等对称函数. 由引理中的假定, 可得

$$|s_h-s_h'|\leqslant Q^{h-1},\quad 1\leqslant h\leqslant k. \tag{1}$$

由 (1) 我们可以证出

$$|\sigma_h-\sigma_h'|\leqslant\begin{cases}1 & h=1,\\ \dfrac{3}{4}(2kQ)^{h-1}, & 2\leqslant h\leqslant k.\end{cases} \tag{2}$$

事实上, 当 $h=1$ 时, (2) 式显然真实. 今假定 (2) 式对 $1,2,\cdots,h-1$ 都真实. 引用关于对称函数习知之公式

$$s_h-\sigma_1s_{h-1}+\sigma_2s_{h-2}-\cdots-(-1)^hh\sigma_h=0$$

及

$$s_h'-\sigma_1's_{h-1}'+\sigma_2's_{h-2}'-\cdots-(-1)^hh\sigma_h'=0.$$

由于 $|\sigma_v|\leqslant\binom{k}{v}Q^v,|s_v|\leqslant kQ^v$, 所以当 $1\leqslant v<h$

$$\begin{aligned}|\sigma_vs_{h-v}-\sigma_v's_{h-v}'|&\leqslant|\sigma_v-\sigma_v'|\ |s_{h-v}|+|\sigma_v'|\ |s_{h-v}-s_{h-v}'|\\&\leqslant\left((2k)^{v-1}k+\binom{k}{v}\right)Q^{h-1}\leqslant\left(1+\frac{1}{v!}\right)(2k)^{v-1}kQ^{h-1}.\end{aligned}$$

当 $h\geqslant 2$ 时, 我们得出

$$\begin{aligned}|\sigma_h-\sigma_h'|&\leqslant\frac{1}{h}\left(1+2k+\frac{3}{2}k\sum_{v=2}^{h-1}(2k)^{v-1}\right)Q^{h-1*}\\&\leqslant\frac{1}{2}\left(1+\frac{1}{2}k+\frac{3}{2}k\frac{(2k)^{h-1}}{2k-1}\right)Q^{h-1}\leqslant\frac{3}{4}(2k)^{h-1}Q^{h-1}.\end{aligned}$$

对适合 $|X| \leqslant Q$ 的 X, 有

$$\begin{aligned}\psi(X) &= |(X-x_1)\cdots(X-x_k)-(X-y_1)\cdots(X-y_k)| \\ &\leqslant \sum_{h=1}^{k}|\sigma_h-\sigma_h'|\,|X|^{k-h} \leqslant \left(1+\frac{3}{4}\sum_{h=2}^{k}(2k)^{h-1}\right)Q^{k-1} \\ &= \left(\frac{1}{4}+\frac{3}{4}\frac{(2k)^k}{2k-1}\right)Q^{k-1}.\end{aligned}$$

由于 $|y_k-x_v| \geqslant R(v=1,2,\cdots,k-1)$, 故得出

$$\begin{aligned}R^{k-1}|y_k-x_k| &\leqslant |(y_k-x_1)(y_k-x_2)\cdots(y_k-x_k)| = \psi(y_k) \\ &\leqslant \left(\frac{1}{4}+\frac{3}{4}\frac{(2k)^k}{2k-1}\right)Q^{k-1} \leqslant 2(2kQ)^{k-1}.\end{aligned}$$

由此可见, 适合引理要求的 x_k 的个数 $\leqslant 2(2kH)^{k-1}$. 对一已定的 x_k

$$x_1^h+\cdots+x_{k-1}^h, \quad 1 \leqslant h \leqslant k-1,$$

在长度 $\leqslant Q^{h-1}(1 \leqslant h \leqslant k-1)$ 的隔间中. 由归纳法的假定, $x_1,\cdots,x_{k-1}$ 的组数

$$\leqslant 2^{k-1}(2(k-1)H)^{\frac{1}{2}(k-1)(k-2)}.$$

由于

$$(2(k-1)H)^{\frac{1}{2}(k-1)(k-2)}(2kH)^{k-1} \leqslant (2kH)^{\frac{1}{2}k(k-1)},$$

即得出本引理.

引理 4.2　命 $c \geqslant 1$. 在引理 4.1 的假定下, 整数组 $x_1,\cdots,x_k$ 中, 使

$$x_1^h+\cdots+x_k^h, \quad 1 \leqslant h \leqslant k$$

在长不超过 $cQ^{(1-1/k)h}(1 \leqslant h \leqslant k)$ 中的组数不超过

$$(4c)^k(2kH)^{\frac{1}{2}k(k-1)}Q^{\frac{1}{2}(k-1)}.$$

证　把第 h 个隔间分成

$$[cQ^{h(1-1/k)}/Q^{h-1}]+1$$

---

* 当 $h=2$ 时, 和号 $\sum\limits_{v=2}^{1}$ 表零.

份, 而对每一份都应用引理 4.1. 由于

$$\prod_{h=1}^{k}\left(\left[\frac{cQ^{h(1-1/k)}}{Q^{h-1}}\right]+1\right)\leqslant\prod_{h=1}^{k}(2cQ^{h(1-1/k)-(h-1)})=(2c)^kQ^{\frac{1}{2}(k-1)},$$

所以至多有 $(2c)^kQ^{\frac{1}{2}(k-1)}$ 组分隔间, 其中之任一都适合引理 4.1. 而对每一组分隔间至多有 $2^k(2kH)^{\frac{1}{2}k(k-1)}$ 组解, 所以得出本引理.

引理 4.3 一组整数 $(g_1,\cdots,g_b), 1\leqslant g_v\leqslant H$, 如适合次之条件谓之佳位组: 其中至少有 k 个, 记之为 $g_{i_1},\cdots,g_{i_k}$, 适合

$$g_{i_{v+1}}-g_{i_v}>1,\quad 1\leqslant v\leqslant k-1.$$

非佳位组的个数最多是

$$H^{k-1}(2(k-1))^b.$$

证 令

$$\{g_1,\cdots,g_b\}$$

为一非佳位组. 命 G_1 为其中之最小整数; G_2 为其中大于 G_1+1 的最小整数; G_3 为其中大于 G_2+1 的最小整数; $\cdots$; 于是得到一个整数列

$$G_1,G_2,\cdots,G_{n-1}.$$

易见 $n<k$, 而任何 g 必等于某一 G_i 或 G_i+1.

因每一个 G 至多能取 H 个值, 故至多只能有 H^{k-1} 个整数列

$$G_1,G_2,\cdots,G_n.$$

又当 $G_1,G_2,\cdots,G_n$ 取定后, 此时每一 g 至多能取 $2(k-1)$ 个值, 因此引理得证.

§4.3 定理的证明

引理 4.4 (递推公式). 命 b 表一 $\geqslant\frac{1}{4}k(k+1)+k$ 的整数, 又命

$$\eta=\left[\frac{1}{k}\frac{\log Q}{\log 2}\right],\quad a=\frac{1}{k},$$

则

$$\int_0^1\cdots\int_0^1|C_k(Q)|^{2b}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\leqslant(5b)^{5b}\max(1,\eta^2)Q^{2k-\frac{1}{2}(k+1)+2(b-k)a}$$
$$\times\int_0^1\cdots\int_0^1|C_k(Q^{1-a})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.$$

证　1) 假定 $\eta \geqslant 2$, 命 s 表一适合 $1 \leqslant s \leqslant \eta - 1$ 的整数. 分 $C_k(Q)$ 为 2^s 部分，每分之长度 $R_s = Q2^{-s}$:

$$C_k(Q) = \sum_{g=1}^{2^s} \sum_{(g-1)R_s < x \leqslant gR_s} \mathrm{e}^{2\pi \mathrm{i} f(x)} = \sum_{g=1}^{2^s} Z_{sg} \text{ (定义)}.$$

命 $Z = (C_k(Q))^b$, 则

$$Z = \sum^{2^{sb}} Z_{sg_1} \cdots Z_{sg_b}, \tag{1}$$

此处 $\sum^{M}$ 表一和，其项数最多是 M(今后将常有此种了解). 又简书

$$Z_s = Z_{s;g_1,\cdots,g_b} = Z_{zg_1 \cdots Z_{sg_b}}. \tag{2}$$

如果 $g_1, \cdots, g_b$ 成一佳位组, 则 $Z_s; g_1, \cdots, g_b$ 称为佳位和, 而以 Z'_s 表之. 由引理 4.3, 非佳位和的个数不超过 $(2(k-1))^b 2^{s(k-1)}$. 把非佳位和 Z_s 中的每一因子分为二份. 如此从一个非佳位和 Z_s 得出 2^b 个和 Z_{s+1}. 由 Z_s 中所得的佳位的 Z_{s+1} 的个数显然不超过

$$(2(k-1))^b 2^{s(k-1)} \cdot 2^b = (4(k-1))^b 2^{s(k-1)}.$$

佳位的 Z_{s+1} 用 Z'_{s+1} 表之. 再如前法, 分割非佳位的和. 由于 Z_1 一定是非佳位的, 所以我们能够开始. 重复此项手续, 由 $s = 1, 2, \cdots$, 到 $\eta - 1$, 而用 Z'_η 表所有的由非佳位的 $Z_{\eta-1}$ 所获得的 Z_η. 于是得

$$Z = \sum_{s=1}^{\eta} \sum^{M_s} Z'_s, \tag{3}$$

此处 $M_s = (4(k-1))^b 2^{s(k-1)}$.

2) 由 Schwarz 不等式可得

$$|C_k(Q)|^{2b} = |Z|^2 \leqslant \eta \sum_{s=1}^{\eta} \left| \sum^{M_s} Z'_s \right|^2 \leqslant \eta \sum_{s=1}^{\eta} M_s \sum^{M_s} |Z'_s|^2. \tag{4}$$

我们可假定 $Z'_{s;g_1,\cdots,g_b} (1 \leqslant s \leqslant \eta - 1)$ 的 $g_1, \cdots, g_k$ 适合引理 4.1 的要求. 不然只须重排足码即可. 因为几何中项不超过代数中项, 所以

$$|Z_{sg_{k+1}} \cdots Z_{sg_b}|^2 \leqslant \frac{1}{b-k} \sum_{i=k+1}^{b} |Z_{sg_i}|^{2(b-k)}. \tag{5}$$

把 $Z_{sg_i}(k+1\leqslant i\leqslant b)$ 分成

$$[Q2^{-s}/Q^{1-a}]+1\leqslant Q^a2^{1-s}$$

(因为 $4\leqslant 2^\eta\leqslant Q^a$) 部分, 每一份的形式是

$$C^*=\sum_x \mathrm{e}^{2\pi\mathrm{i}f(x)},$$

此处 x 经过一长 $\leqslant Q^{1-a}$ 的隔间; 即有一整数 ω 存在, 使

$$\omega<x\leqslant\omega+Q',\quad 0<Q'\leqslant Q^{1-a},\quad 0\leqslant\omega\leqslant g_iR_s\leqslant Q.$$

利用 Hölder 不等式可知

$$|Z_{sg_i}|^{2(b-k)}\leqslant\left(\sum^{Q^a2^{1-s}}|C^*|\right)^{2(b-k)}\leqslant(Q^a2^{1-s})^{2(b-k)-1}\sum^{Q^a2^{1-s}}|C^*|^{2(b-k)}.\tag{6}$$

由 (4), (5) 及 (6) 可得出

$$|Z|^2\leqslant\frac{\eta}{b-k}\sum_{s=1}^{\eta}M_s(Q^a2^{1-s})^{2(b-k)-1}\sum^{N_s}|Z_{sg_1}|^2\cdots|Z_{sg_k}|^2\ |C^*|^{2(b-k)},\tag{7}$$

此处 $N_s=M_s(b-k)Q^a2^{1-s}=(4(k-1))^b\cdot 2^{s(k-1)}(b-k)Q^a2^{1-s}$. 过 k 维单位方体 $(0\leqslant\alpha_1\leqslant 1,\cdots,0\leqslant\alpha_k\leqslant 1)$ 求积分, 得出

$$\begin{aligned}&\int_0^1\cdots\int_0^1|Z|^2\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant&\frac{\eta}{b-k}\sum_{s=1}^{\eta}M_s(Q^a2^{1-s})^{2(b-k)-1}\\ &\times\sum^{N_s}\int_0^1\cdots\int_0^1|Z_{sg_1}|^2\cdots|Z_{sg_k}|^2|C^*|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.\end{aligned}\tag{8}$$

3) 积分

$$\int_0^1\cdots\int_0^1|Z_{sg_1}|^2\cdots|Z_{sg_k}|^2|C^*|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\tag{9}$$

等于下列方程组的解答数:

$$\begin{aligned}&x_1^h+\cdots+x_k^h+y_1^h+\cdots+y_{b-k}^h\\ =&x_1'^h+\cdots+x_k'^h+y_1'^h+\cdots+y_{b-k}'^h,\quad 1\leqslant h\leqslant k,\end{aligned}$$

此处变数 y 及 y' 在形如

$$\omega < y, y' \leqslant \omega + Q', \quad 0 < Q' \leqslant Q^{1-a},\ 0 \leqslant \omega \leqslant Q$$

的隔间中, 而 x 及 x' 在隔间

$$(g_i - 1)R_s < x_i, x_i' \leqslant g_i R_s$$

之中, 而 $s \leqslant \eta - 1$, 整数 $g_1, \cdots, g_k$ 适合于引理 4.1 的条件.

以 $X + \omega$ 及 $Y + \omega$ 各代 x 及 y. 则 (9) 式也就是方程组

$$\begin{aligned} &X_1^h + \cdots + X_k^h + Y_1^h + \cdots + Y_{b-k}^h \\ =&X_1'^h + \cdots + X_k'^h + Y_1'^h + \cdots + Y_{b-k}'^h, \quad 1 \leqslant h \leqslant k \end{aligned} \tag{10}$$

的解数, 此处诸 Y 在隔间 $(0, Q')$ 之中, 而 X_i 及 X_i' 在

$$-\omega + (g_i - 1)R_s < X_i, X_i' \leqslant -\omega + g_i R_s, \quad 0 \leqslant \omega \leqslant Q \tag{11}$$

之中.

若先固定了 X', 则 X 适合于引理 4.2 的条件: 其中 $c = 2(b-k)$ 及 $H = 2^s$. 所以 X 及 X' 的组数不超过

$$\begin{aligned} &R_s^k \{8(b-k)\}^k (2k2^s)^{\frac{1}{2}k(k-1)} Q^{\frac{1}{2}(k-1)} \\ =&\{8(b-k)\}^k (2k)^{\frac{1}{2}k(k-1)} 2^{\frac{1}{2}sk(k-1) - sk} Q^{2k - \frac{1}{2}(k+1)}. \end{aligned} \tag{12}$$

又对已定的 X 及 X',Y 及 Y' 的组数不超过

$$\int_0^1 \cdots \int_0^1 |C_k(Q^{1-a})|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k$$

$\left(由于 \left|\int_0^1 f(x) \mathrm{e}^{\mathrm{i}xy} \mathrm{d}x\right| \leqslant \int_0^1 |f(x)| \mathrm{d}x\right)$. 所以, 当 $1 \leqslant s \leqslant \eta - 1$ 时,

$$\begin{aligned} &\int_0^1 \cdots \int_0^1 |Z_{sg_1} \cdots Z_{sg_k}|^2 |C^*|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \\ \leqslant&(8(b-k))^k (2k)^{\frac{1}{2}k(k-1)} 2^{\frac{1}{2}sk(k+1) - 2sk} Q^{2k - \frac{1}{2}(k+1)} \\ &\times \int_0^1 \cdots \int_0^1 |C_k(Q^{1-a})|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k. \end{aligned} \tag{13}$$

当 $s = \eta$ 时, 我们用极显然的不等式:

$$\int_0^1 \cdots \int_0^1 |Z_{sg_1} \cdots Z_{sg_k}|^2 |C^*|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k$$

$$\leqslant R_\eta^{2k}\int_0^1\cdots\int_0^1|C_k(Q^{1-a})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k. \tag{14}$$

由于 $\eta+1\geqslant \log Q/k\log 2$, 所以 $Q2^{-\eta k}\leqslant 2^k$. 又因为

$$\begin{aligned}R_\eta^{2k}&=Q^{2k}2^{-2k\eta}\\&=2^{-\eta\left[2k-\frac{1}{2}k(k+1)\right]}Q^{2k-\frac{1}{2}(k+1)}(Q2^{-\eta k})^{\frac{1}{2}(k+1)}\\&\leqslant 2^{-\eta\left[2k-\frac{1}{2}k(k+1)\right]}Q^{2k-\frac{1}{2}(k+1)}2^{\frac{1}{2}k(k+1)}.\end{aligned}$$

可知 (13) 式对 $s=\eta$ 仍真实.

4) 结合 (8) 及 (13)(当 $s=1,2,\cdots,\eta$), 可得

$$\begin{aligned}&\int_0^1\cdots\int_0^1|C_k(Q)|^{2b}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\&\leqslant\frac{\eta}{b-k}\sum_{s=1}^{\eta}M_s(Q^a2^{1-s})^{2(b-k)-1}N_s(8(b-k))^k\\&\quad\times(2k)^{\frac{1}{2}k(k-1)}2^{\frac{1}{2}sk(k+1)-2sk}Q^{2k-\frac{1}{2}(k+1)}\int_0^1\cdots\int_0^1|C_k(Q^{1-a})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\&\leqslant\eta c\sum_{s=1}^{\eta}2^{-s(2b-\frac{1}{2}k(k+1)-2k)}Q^{2k-\frac{1}{2}(k+1)+2(b-k)}aQ^{2k-\frac{1}{2}(k+1)+2(b-k)a}\\&\quad\times\int_0^1\cdots\int_0^1|C_k(Q^{1-a})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\&\leqslant\eta^2cQ^{2k-\frac{1}{2}(k+1)+2(b-k)a}\int_0^1\cdots\int_0^1|C_k(Q^{1-a})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k,\end{aligned}\tag{15}$$

此处用了不等式 $2b\geqslant\dfrac{1}{2}k(k+1)+2k$, 式中之

$$c=(4(k-1))^{2b}2^{2(b-k)}(8b)^k(2k)^{\frac{1}{2}k(k-1)}.$$

由于

$$c<(4b)^{2b}2^{2b}(8b)^b(2b)^{2b}\leqslant((8b)^2\cdot 8b\cdot(2b)^2)^b\leqslant(5b)^{5b},$$

所以本定理当 $\eta\geqslant 2$ 时真实.

5) 假定 $\eta<2$. 则

$$\frac{1}{k}\log Q/\log 2<2,\quad 即\ Q<4^k.$$

把 $C_k(Q)$ 分为四份, 每一份的形式如

$$C^*=\sum_{\omega<x\leqslant\omega+Q'}\mathrm{e}^{2\pi\mathrm{i}f(x)},\quad 0<Q'\leqslant\frac{1}{4}Q\leqslant Q^{1-a}.$$

用 Hölder 不等式得出

$$|C_k(Q)|^{2b} \leqslant 4^{2b-1}\sum^4 |C^*|^{2b} \leqslant 4^{2b-1}Q^{2k(1-a)}\sum^4 |C^*|^{2(b-k)}.$$

在 k 维单位方体上求积分, 得出

$$\begin{aligned}&\int_0^1\cdots\int_0^1 |C_k(Q)|^{2b}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant&4^{2b-1}Q^{2k(1-a)}\sum^4\int_0^1\cdots\int_0^1 |C^*|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant&4^{2b}Q^{2k(1-a)}\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant&4^{2b}Q^{2k-\frac{1}{2}(k+1)+2(b-k)a}\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k,\end{aligned}$$

此处用了 $2b > \frac{1}{2}k(k+1)$. 故得出引理 4.4.

定理 5′　仍如定理 5 的假定, 若 $s \geqslant \frac{1}{4}k(k+1)+lk$, 则

$$\int_0^1\cdots\int_0^1 |C_k(P)|^{2s}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k \leqslant (5s)^{5sl}(\log P)^{2l}P^{2s-\frac{1}{2}k(k+1)+\delta}.$$

这定理显然是定理 5 的更精密的形式.

证　如命 $P^{1-a}\leqslant 3$, 则 $P\leqslant 9$, 而本定理毋须证明. 我们假定 $P^{1-a}>3$. 则 $P>e$.

当 $l=0$ 时, 定理显然真实. 今在 l 上用归纳法. 假定此结论对 $l-1$ 真实. 由引理 4.4 可知

$$\begin{aligned}&\int_0^1\cdots\int_0^1 |C_k(P)|^{2s}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant&(5s)^{5s}P^{2k-\frac{1}{2}(k+1)+2(s-k)a}\\ &\times(\log P)^2\int_0^1\cdots\int_0^1 |C_k(P^{1-a})|^{2(s-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.\end{aligned}\tag{16}$$

用归纳法的假定, 取 $l-1, s-k$ 及 P^{l-a} 代替 l, s 及 P, 可知当 $P^{1-a}>3>2$ 时,

$$\begin{aligned}&\int_0^1\cdots\int_0^1 |C_k(P^{1-a})|^{2(s-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant&(5s)^{5s(l-1)}(\log P)^{2(l-1)}\\ &\times P^{(1-a)(2s-2k-\frac{1}{2}k(k+1)+\frac{1}{2}k(k+1)(1-a)^{l-1})}.\end{aligned}\tag{17}$$

由 (16) 及 (17) 总结出本定理.

§4.4　推　论

定理 6　命 $P \geqslant 2, s \geqslant \frac{1}{4}k(k+1)+lk$. 又命 $f(x)$ 表一 k 次的整值多项式, 则

$$\int_0^1 \left|\sum_{x=1}^{P} e(\alpha f(x))\right|^{2s} \mathrm{d}\alpha \ll (\log P)^{2l} P^{2s-k+\delta},$$

此处

$$\delta = \frac{1}{2}k(k+1)(1-a)^l.$$

证　如第三章定理 4 的证明, 我们可以假定 $f(x)$ 是一整系数多项式:

$$f(x) = A_k x^k + \cdots + A_1 x + A_0.$$

方程

$$f(x_1)+\cdots+f(x_s) = f(y_1)+\cdots+f(y_s), \quad 1 \leqslant x,\ y \leqslant P$$

的整数解之组数显然等于方程组

$$x_1^h+\cdots+x_s^h-y_1^h-\cdots-y_s^h = N_h, \quad 1 \leqslant h \leqslant k \tag{1}$$

的解数, 此处 $N_1, \cdots, N_k$ 适合于

$$A_k N_k + \cdots + A_1 N_1 = 0, \quad N_h \ll P^h \tag{2}$$

(注意 $x_1, \cdots, x_s, y_1, \cdots, y_s, N_1, \cdots, N_k$ 都视为未知数).

由于 $N_h \ll P^h$, 所以有

$$\ll P^{l+2+\cdots+k-1} \ll P^{\frac{1}{2}k(k-1)}$$

组 $N_1, \cdots, N_k$ 适合 (2) 式, 因为 N_k 是由 $N_1, \cdots, N_{k-1}$ 唯一地决定.

对固定的 $N_1, \cdots, N_{k-1}$ 及 N_k, (1) 式的解数等于

$$\int_0^1 \cdots \int_0^1 \left|\sum_{x=1}^{P} e(\alpha_k x^k + \cdots + \alpha_1 x)\right|^{2s} e(-(N_k\alpha_k+\cdots+N_1\alpha_1))\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.$$

由定理 5′, 此积分

$$\begin{aligned}&\leqslant \int_0^1 \cdots \int_0^1 \left|\sum_{x=1}^{P} e(\alpha_k x^k + \cdots + \alpha_1 x)\right|^{2s} \mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k \\ &\leqslant (5s)^{5sl}(\log P)^{2l} P^{2s-\frac{1}{2}k(k+1)+\delta}.\end{aligned}$$

§4.5

在隔间 $a<x<b$ 上定义的实函数 $f(x)$, 如对隔间中的任何三点 $x_1<x_2<x_3$, 常有下之不等式:

$$f(x_2) \leqslant \frac{(x_3-x_2)f(x_1)+(x_2-x_1)f(x_3)}{x_3-x_1},$$

则称 $f(x)$ 为 (a,b) 上的凸函数.

引理 4.5　设 $x_1<x_2<x_3$ 是隔间 $a<x<b$ 中的已给三点. $\alpha,\beta,0<\lambda\leqslant 1$ 是已给三数. 并设 $f(x)$ 是隔间 (a,b) 上适合条件

$$\begin{cases} f(x_1)\leqslant \alpha, \\ f(x_3)\leqslant \beta+\lambda f(x_2) \end{cases}$$

的一个凸函数. 则有

$$f(x_2) \leqslant \frac{\alpha(x_3-x_2)+\beta(x_2-x_1)}{x_3-x_1-\lambda(x_2-x_1)}. \tag{1}$$

证　由凸函数的定义及引理的假设, 可得

$$f(x_2) \leqslant \frac{(x_3-x_2)f(x_1)+(x_2-x_1)f(x_3)}{x_3-x_1} \leqslant \frac{\alpha(x_3-x_2)+(\beta+\lambda f(x_2))(x_2-x_1)}{x_3-x_1}.$$

上式移项并整理之, 立得 (1) 式.

引理 4.6　当 $v\geqslant 0$ 时, 定义 $g(v)$ 为

$$\log\left(\int_0^1\cdots\int_0^1 |C_k(Q)|^{2v}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right)\Big/\log Q. \tag{2}$$

当 Q 在隔间 $Q_0\leqslant Q<\infty$ 中变动时之最小上界, 则 $g(v)$ 为 v 在隔间 $(0,\infty)$ 上之一凸函数. 于此, Q_0 是任一给定的正常数.

证　设 $v_2>v_1\geqslant 0$ 是任意二数, 则当 $0<t<1$ 时, $v_1t+v_2(1-t)$ 即表区间 $v_1<v<v_2$ 中之任意一点. 如能证明

$$g(v_1t+v_2(1-t)) \leqslant tg(v_1)+(1-t)g(v_2), \tag{3}$$

则引理得证.

由引理 3.1 可知

$$\frac{\displaystyle\int_0^1\cdots\int_0^1 |C_k|^{2(v_1t+v_2(1-t))}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k}{\left(\displaystyle\int_0^1\cdots\int_0^1 |C_k|^{2v_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right)^t\left(\displaystyle\int_0^1\cdots\int_0^1 |C_k|^{2v_2}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right)^{1-t}}$$

$$=\int_0^1\cdots\int_0^1\left(\frac{|C_k|^{2v_1}}{\int_0^1\cdots\int_0^1|C_k|^{2v_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k}\right)^t\left(\frac{|C_k|^{2v_2}}{\int_0^1\cdots\int_0^1|C_k|^{2v_2}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k}\right)^{1-t}$$
$$\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k$$
$$\leqslant\int_0^1\cdots\int_0^1\left(\frac{t|C_k|^{2v_1}}{\int_0^1\cdots\int_0^1|C_k|^{2v_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k}+\frac{(1-t)|C_k|^{2v_2}}{\int_0^1\cdots\int_0^1|C_k|^{2v_2}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k}\right)$$
$$\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k$$
$$=t+(1-t)=1.$$

由上式可以立刻得出 (3) 式.

引理 4.7 设 $k\geqslant 2, u_0$ 是一正整数, Q_0' 为一仅与 k 有关之常数. 并设当 $Q\geqslant Q_0'$ 时,

$$\int_0^1\cdots\int_0^1|C_k(Q)|^{2u_0}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\leqslant Q^{v_0},\tag{4}$$

则对任一整数 $u\geqslant\max\left(\frac{1}{4}k(k+1),u_0+1\right)$ 及 $\varepsilon>0$, 我们有

$$\int_0^1\cdots\int_0^1|C_k(Q)|^{2u}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\leqslant b(k,u_0,v_0,u,\varepsilon)Q^{2u-\frac{1}{2}k(k+1)+\delta+\varepsilon},\tag{5}$$

此处

$$\delta=\frac{k^2(2v_0-4u_0+k^2+k)}{2(k^2+u-u_0)}.\tag{6}$$

证 由引理 4.4 知当 $Q\geqslant Q_0''(k,u,\varepsilon')$ 时,

$$\int_0^1\cdots\int_0^1|C_k(Q)|^{2(u+k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k$$
$$\leqslant Q^{2k-\frac{1}{2}(k+1)+2ua+\varepsilon'}$$
$$\times\int_0^1\cdots\int_0^1|C_k(Q^{1-a})|^{2u}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.$$

今取 $Q_0=\max(Q_0',Q_0'')$, 并命 $g(v)$ 如 (2) 所定义. 则有 $Q'\geqslant Q_0$, 使

$$g(u+k)\leqslant\log\left(\int_0^1\cdots\int_0^1|C_k(Q')|^{2(u+k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right)\Big/\log Q'+\varepsilon'$$
$$\leqslant\left(2k-\frac{1}{2}(k+1)+2ua+2\varepsilon'\right)$$
$$+\log\left(\int_0^1\cdots\int_0^1|C_k(Q'^{1-a})|^{2u}\mathrm{d}\alpha_1\cdots d\alpha_k\right)\Big/\log Q'$$

$$\leqslant 2k - \frac{1}{2}(k+1) + 2ua + 2\varepsilon' + (1-a)g(u).$$

由于 $g(v)$ 是一凸函数, 又 $u_0 < u < u+k$, 故由引理 4.5 可得

$$\begin{aligned} g(u) &\leqslant \frac{v_0(u+k-u) + \left(2k - \frac{1}{2}(k+1) + 2ua + 2\varepsilon'\right)(u-u_0)}{u+k-u_0-(1-a)(u-u_0)} \\ &= \frac{2k^2v_0 + (3k^2-k+4u)(u-u_0) + \varepsilon''}{2(k^2+u-u_0)} \\ &\leqslant 2u - \frac{1}{2}k(k+1) + \frac{k^2(2v_0-4u_0+k^2+k)}{2(k^2+u-u_0)} + \varepsilon. \end{aligned}$$

由此即得引理.

第 5 章　某些三角和的中值定理 (II)

§5.1

定理 7(定理 B_k)　设 P 是一正整数,

$$C_k=\sum_{x=1}^{P} e(\alpha_k x^k+\cdots+\alpha_1 x),$$

则

$$\int_0^1\cdots\int_0^1 |C_k|^\lambda \mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k \leqslant C_1(k,\varepsilon)P^{\lambda-\frac{1}{2}k(k+1)+\varepsilon},$$

此处 $\lambda=\lambda(k)$ 的数值由下面的表来定义:

k	2	3	4	5	6	7	8	9	10
λ	6	16	46	110	240	414	672	1080	1770

当 $k=2$ 时, 我们有较精密的结果 (定理 B_2'):

$$\int_0^1\int_0^1\left|\sum_{x=1}^{P} e(\alpha_2 x^2+\alpha_1 x)\right|^6 \mathrm{d}\alpha_1\mathrm{d}\alpha_2 \leqslant b_1 P^3(\log P)^3.$$

此定理的证明依赖于下面的定理:

定理 8(定理 A_k)　命

$$f(x)=\alpha_0 x^k+\alpha_1 x^{k-1}+\cdots,$$

此处 a_0 代表一个绝对值 $\leqslant b_2(k)$ 的整数, α_1 是一个绝对值不超过 $b_3(k)P$ 的整数. 又命

$$S_k=\sum_{x=1}^{P} e(\alpha_k f(x)+\alpha_{k-2}x^{k-2}+\cdots+\alpha_1 x),$$

则

$$\int_0^1\cdots\int_0^1 |S_k|^\lambda \mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_{k-2}\mathrm{d}\alpha_k \leqslant c_2(k,\varepsilon)P^{\lambda-\frac{1}{2}(k^2-k+2)+\varepsilon},$$

此处 $\lambda=\lambda(k)$ 的数值由下面的表来定义:

k	3	4	5	6	7	8	9	10
λ	10	32	86	208	354	544	826	1258

这两条定理的证明互相依赖; 就是说, 我们用定理 $A_{l_1}(l_1 \leqslant k-1)$ 及 $B_{l_2}(l_2 \leqslant k-1)$ 来证明 A_k; 再由定理 $A_{l_1(l_1\leqslant k)}$ 及 $B_{l_2}(l_2 \leqslant k-1)$ 来证明 B_k. 对不同的 k, 方法上略有变化. 当然, 如果用归纳法, 我们可有一个一致性的方法, 但得出的结果稍欠精密. 因此, 我们运用这个各阶段不相同的方法.

§5.2　定理 A_k(即定理 8) 的注记

在定理 A_k 中我们可以取 $f(x)=x^k$. 其证法如: 积分

$$\int_0^1 \cdots \int_0^1 |S_k|^{2\mu} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_{k-2} \mathrm{d}\alpha_k$$

之值等于方程式组

$$\begin{gathered} f(x_1)+\cdots+f(x_\mu)=f(y_1)+\cdots+f(y_\mu), \\ x_1^h+\cdots+x_\mu^h=y_1^h+\cdots+y_\mu^h, \quad 1 \leqslant h \leqslant k-2, \\ 1 \leqslant x_\nu \leqslant P, \quad 1 \leqslant y_\nu \leqslant P \end{gathered}$$

的整数解答 $x_1,\cdots,x_\mu,y_1,\cdots,y_\mu$ 的组数. 不妨假定 $a_0>0$. 各以 $a_0^{k-1}k^k, a_0^h k^h(1 \leqslant h \leqslant k-2)$ 乘以上诸式, 即得

$$\sum_{\nu=1}^{\mu}\{(a_0kx_\nu)^k+ka_1(a_0kx_\nu)^{k-1}+\cdots\}=\sum_{\nu=1}^{\mu}\{(a_0ky_\nu)^k+ka_1(a_0ky_\nu)^{k-1}+\cdots\},$$

$$\sum_{\nu=1}^{\mu}(a_0kx_v)^h=\sum_{\nu=1}^{\mu}(a_0ky_v)^h, \quad 1 \leqslant h \leqslant k-2.$$

命 $x_v'=a_0kx_v+a_1$ 及 $y_v'=a_0ky_v+a_1$, 则得方程组

$$\begin{aligned} & x_1'^k+\cdots+x_\mu'^k=y_1'^k+\cdots+y_\mu'^k, \\ & x_1'^h+\cdots+x_\mu'^h=y_1'^h+\cdots+y_\mu'^h, \quad 1 \leqslant h \leqslant k-2, \end{aligned} \tag{1}$$

但其中

$$k|(x_\nu'-a_1), \quad k|(y_\nu'-a_1).$$

由是得出

$$\int_0^1 \cdots \int_0^1 |S_k|^{2\mu} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_{k-2} \mathrm{d}\alpha_k$$

$$\leqslant \int_0^1 \cdots \int_0^1 \left| \sum_{x=a_1}^{a_0kP+a_1} e(\alpha_k x^k + \alpha_{k-2}x^{k-2} + \cdots + \alpha_1 x) \right|^{2\mu} d\alpha_1 \cdots d\alpha_{k-2} d\alpha_k$$

$$\leqslant 2^{2\mu-1}\left(\int_0^1 \cdots \int_0^1 \left| \sum_{a_1 \leqslant x \leqslant -1} e(\alpha_k x^k + \alpha_{k-2}x^{k-2} + \cdots + \alpha_1 x) \right|^{2\mu} d\alpha_1 \cdots d\alpha_{k-2} d\alpha_k \right.$$

$$\left. + \int_0^1 \cdots \int_0^1 \left| \sum_{x=0}^{a_0kP+a_1} e(\alpha_k x^k + \alpha_{k-2}x^{k-2} + \cdots + \alpha_1 x) \right|^{2\mu} d\alpha_1 \cdots d\alpha_{k-2} d\alpha_k \right)^*$$

$$\ll \int_0^1 \cdots \int_0^1 \left| \sum_{x}^{P} e(\alpha_k x^k + \alpha_{k-2}x^{k-2} + \cdots + \alpha_1 x) \right|^{2\mu} d\alpha_1 \cdots d\alpha_{k-2} d\alpha_k + 1,$$

此处用上 $a_0 \ll 1$ 及 $a_1 \ll P$. 因之, 我们仅需考察 $f(x) = x^k$ 的情况.

§5.3

我们现在的目的在证明:

$$\int_0^1 \cdots \int_0^1 |S_k|^{2k} d\alpha_1 \cdots d\alpha_{k-2} d\alpha_k \leqslant b_4(k) P^k L^{k(2^{k-1}-1)}$$

及

$$\int_0^1 \cdots \int_0^1 |C_k|^{2(k+1)} d\alpha_1 \cdots d\alpha_k \leqslant b_5(k) P^{k+1} L^{2^k-1},$$

此处 $L = \log P$.

引理 5.1　命

$$s_v = x_1^v + \cdots + x_k^v, \quad 1 \leqslant v \leqslant k.$$

对称函数

$$f = (s_1 - x_1) \cdots (s_1 - x_k)$$

可以表成 $s_1, \cdots, s_{k-2}$ 及 s_k 的函数而与 s_{k-1} 无关.

证　命 σ_i 表 $x_1, \cdots, x_k$ 的 i 次初等对称函数, 则

$$f = s_1^k - \sigma_1 s_1^{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k \sigma_k.$$

由与对称函数有关的一条习知的定理, 可得

$$f = (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k\sigma_k + f_1(s_1, \cdots, s_{k-2}). \tag{1}$$

* 若 $a_1 > -1$, 则第一个积分空无所有, 以 0 代之. 又若 $a_0kP + a_1 < 0$, 则第二个积分也以 0 代之.

由与对称函数有关的牛顿定理, 可知

$$(-1)^k k\sigma_k = -s_k + \sigma_1 s_{k-1} + (-1)^k \sigma_{k-1} s_1 + f_2(s_1, \cdots, s_{k-2})$$

及

$$(-1)^{k-1}(k-1)\sigma_{k-1} = -s_{k-1} + f_3(s_1, \cdots, s_{k-2}).$$

由此推得

$$\begin{aligned} & k((-1)^k\sigma_k + (-1)^{k-1}\sigma_{k-1}s_1) \\ =& -s_k + \sigma_1 s_{k-1} + (-1)^k\sigma_{k-1}s_1 + (-1)^{k-1}\sigma_{k-1}s_1 - s_1 s_{k-1} + f_4(s_1, \cdots, s_{k-2}) \\ =& -s_k + f_4(s_1, \cdots, s_{k-2}). \end{aligned} \tag{2}$$

由等式 (1) 及 (2) 可得本引理.

引理 5.2

$$\int_0^1 \cdots \int_0^1 |S_k|^{2k} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_{k-2} \mathrm{d}\alpha_k \leqslant b_4(k) P^k L^{k(2^{k-1}-1)}.$$

证　命 $l = x_1 + \cdots + x_k$. 则由引理 5.1 可知由等式组

$$\left.\begin{aligned} & x_1^k + \cdots + x_k^k = y_1^k + \cdots + y_k^k, \\ & x_1^h + \cdots + x_k^h = y_1^h + \cdots + y_k^h, \quad 1 \leqslant h \leqslant k-2. \end{aligned}\right\} \tag{3}$$

得出

$$(l - x_1) \cdots (l - x_k) = (l - y_1) \cdots (l - y_k). \tag{4}$$

对已予的 $y_1, \cdots, y_k$, 显然

$$(l - y_1) \cdots (l - y_k) \neq 0,$$

$x_1, \cdots x_k$ 的组数最多是

$$\mathrm{d}^{k-1}(|(l - y_1)(l - y_2) \cdots (l - y_k)|).$$

因此 (3) 式的解答之组数 (由于引理 2.5)

$$\begin{aligned} & \ll \sum_{y_1}^{P} \cdots \sum_{y_k}^{P} \mathrm{d}^{k-1}(|(l - y_1) \cdots (l - y_k)|) \\ & \leqslant \sum_{z_1}^{P} \cdots \sum_{z_k}^{P} \mathrm{d}^{k-1}(z_1) \cdots d^{k-1}(z_k) \\ & \leqslant \left(\sum_{z}^{P} \mathrm{d}^{k-1}(z) \right)^k \\ & \ll P^k L^{k(2^{k-1}-1)}. \end{aligned}$$

引理 5.3　由等式组

$$x_1^h+\cdots+x_{k+1}^h=y_1^h+\cdots+y_{k+1}^h,\quad 1\leqslant h\leqslant k, \tag{5}$$

可引导出一形如

$$(x_k-y_1)\cdots(x_k-y_k)=(x_{k+1}-y_{k+1})g(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})$$

之等式, 此处 g 是一 $(k-1)$ 次的齐次多项式, 其中含有 x_{k+1},y_{k+1} 的齐次部分不为 $x_{k+1}-y_{k+1}$ 所整除, 且 g 中 x_{k+1}^{k-1} 的系数不等于 0.

证　命 $s_v=\sum\limits_{j=1}^{k-1}x_j^v$ 及 $t_v=\sum\limits_{j=1}^{k-1}y_j^v$. (5) 式与次式相当

$$s_h=t_h-(x_k^h-y_k^h)-(x_{k+1}^h-y_{k+1}^h),\quad 1\leqslant h\leqslant k. \tag{6}$$

习知

$$s_k-\sigma_1 s_{k-1}+\sigma_2 s_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}s_1=0, \tag{7}$$

此处 $\sigma_i=\sigma_i(x_1,\cdots,x_{k-1})$ 是 $x_1,\cdots,x_{k-1}$ 的 i 次初等对称函数. 习知 $\sigma_1,\cdots,\sigma_{k-1}$ 是可以由 $s_1,\cdots s_{k-1}$ 表出来的. 更确切些, 我们有

$$s_k-s_1 s_{k-1}+\sigma_2(s_1,s_2)s_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}(s_1,\cdots,s_{k-1})s_1=0. \tag{8}$$

同法得出

$$t_k-t_1 t_{k-1}+\sigma_2(t_1,t_2)t_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}(t_1,\cdots,t_{k-1})t_1=0. \tag{9}$$

将 (6) 式代入 (8) 式之左方而得的函数用 $T(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})$ 来表示. 今证明公式

$$T(y_1,\cdots,y_k,x_k,x_{k+1},x_{k+1})=-k(x_k-y_1)\cdots(x_k-y_k).$$

因为当 $x_k=y_k$ 时, 由 (9) 可知上式左端是零, 故 $T(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})$ 含有因子 x_k-y_k. 如命 $t_v=\sum\limits_{\substack{j=1\\ j\neq i}}^{k}y_j^v$, 则同法可知其含有因子 $x_k-y_i(1\leqslant i\leqslant k-1)$. 今 $T(y_1,\cdots,y_k,x_k,x_{k+1},x_{k+1})$ 对 x_k 而言是一 k 次多项式, 比较上式二边 $y_1,\cdots,y_k$ 的系数, 可见等式成立.

由此可知

$$T(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})+k(x_k-y_1)\cdots(x_k-y_k)$$

是一多项式, 当 $x_{k+1}=y_{k+1}$ 时其值是零. 因此

$$\begin{aligned}&k^{-1}T(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})\\=&-(x_k-y_1)\cdots(x_k-y_k)+(x_{k+1}-y_{k+1})g(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1}).\end{aligned}$$

最后, 在将 (6) 代入 (8) 式之左方时, x_{k+1},y_{k+1} 的整次部分的次数是 k, 仅其中之第一项所给与的部分是 $x_{k+1}-y_{k+1}$ 的倍数, 而非 $(x_{k+1}-y_{k+1})^2$ 的倍数. 其他诸项都是 $(x_{k+1}-y_{k+1})^2$ 的倍数. 又易见 $T(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})$ 中 x_{k+1}^k 的系数是 $-k$, 故 g 中 x_{k+1}^{k-1} 的系数是 -1. 因此得出本引理.

引理 5.4

$$\int_0^1\cdots\int_0^1|C_k|^{2(k+1)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\leqslant b_5(k)P^{k+1}L^{2^k-1}.$$

证 引理中不等式左边等于方程组

$$\sum_{v=1}^{k+1}x_v^h=\sum_{v=1}^{k+1}y_v^h,\quad 1\leqslant h\leqslant k,\ 1\leqslant x,\ y\leqslant P \tag{10}$$

的解数. 由引理 5.3 可得

$$(x_k-y_1)\cdots(x_k-y_k)=(x_{k+1}-y_{k+1})g(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1}). \tag{11}$$

若 $(x_k-y_1)\cdots(x_k-y_k)=0$, 则 $x_1,\cdots,x_{k+1}$ 乃由 $y_1,\cdots,y_{k+1}$ 换位而得的. 方程式有 $O(P^{k+1})$ 个解.

命 n 表一整数 $\neq 0$. 且 $n=\lambda_1\cdots\lambda_k=\mu_1\mu_2$. 今考察方程组

$$x_k-y_v=\lambda_v,\quad 1\leqslant v\leqslant k \tag{12}$$

$$x_{k+1}-y_{k+1}=\mu_1 \tag{13}$$

及

$$g(y_1,\cdots,y_k,x_k,y_{k+1},x_{k+1})=\mu_2 \tag{14}$$

的解数.

若已与 $\lambda_1,\cdots,\lambda_k,\mu_1,\mu_2$ 及 x_k, 则由 (12) 式唯一地决定了 $y_1,\cdots,y_k$ 的数值. 再由 (13), (14) 及 g 的性质, 可知适合 (13), (14) 的 x_{k+1},y_{k+1} 最多是 k 对.

但对一已知的 n, 整数组 $\lambda_1,\cdots,\lambda_k,\mu_1,\mu_2$ 的组数 $\leqslant \mathrm{d}^k(n)$. 而由已知的 $\lambda_1,\cdots,\lambda_k,\mu_1,\mu_2$ 及 x_k, (10) 式的解数是 $O(1)$. 因此, (10) 式的解数

$$\ll\sum_{x_k=1}^{P}\sum_{n}^{P^k}\mathrm{d}^k(n)\ll P^{k+1}L^{2^k-1}.$$

此处用了引理 2.5

引理 5.5

$$\int_0^1\cdots\int_0^1|S_k|^{2u}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_{k-2}\mathrm{d}\alpha_k\leqslant(2u+1)P^{k-1}\int_0^1\cdots\int_0^1|C_k|^{2u}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.$$

证　显然有

$$\begin{aligned}\int_0^1\cdots\int_0^1|S_k|^{2u}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_{k-2}\mathrm{d}\alpha_k&\leqslant\sum_{|N|\leqslant uP^{k-1}}\int_0^1\cdots\int_0^1|C_k|^{2u}\mathrm{e}^{-2\pi i\alpha_{k-1}N}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\&\leqslant(2u+1)P^{k-1}\int_0^1\cdots\int_0^1|C_k|^{2u}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.\end{aligned}$$

§5.4

引理 5.6　命 $g_v(x)$ 是 x 的有整数系数的多项式,

$$g(x)=g_1(x)\alpha_1+\cdots+g_s(x)\alpha_s$$

是一 k 次多项式. 命

$$F=\sum_{x=1}^{P}\mathrm{e}^{2\pi i g(x)}.$$

用 Δ^μ 表 $\underset{y_\mu}{\Delta}\cdots\underset{y_1}{\Delta}$, 则当 $\mu=1,2,\cdots,k-1$ 时

$$F^{2^\mu}\ll P^{2^\mu-1}+P^{2^\mu-\mu-1}\sum_{y_1}^{P}\cdots\sum_{y_\mu}^{P}\sum_{x_{\mu+1}}^{P}{}^*e(y_1\cdots y_\mu\Delta^\mu g(x_{\mu+1})),$$

此处 $*$ 表示下面两条件之一: (i)

$$y_1\cdots y_\mu\Delta^\mu g_i(X)$$

恒等于零, 或, (ii)

$$y_1\cdots y_\mu\Delta^\mu g_i(x_{\mu+1})\neq0.$$

证　此引理可由引理 3.3 推出. 因为如果 $y_1\cdots y_\mu\Delta^\mu g_i(X)$ 不恒等于零, 则

$$y_1\cdots y_\mu\Delta^\mu g_i(x_{\mu+1})=0$$

的解数 $\ll P^\mu$.

§5.5　定理的证明

B_2 及 B_2' 已由引理 5.4 直接证明.

A_3 的证明. 由引理 5.6 可得

$$|S_3|^4 \ll P^3 + P \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{x_3}^{P}{}^{*} e(y_1 y_2 \Delta^2(\alpha_3 x_3^3 + \alpha_1 x_3)).$$

以 $|S_3|^6$ 乘此式两边, 再对 α_1 及 α_3 各由 0 到 1 积分, 可得

$$\int_0^1 \int_0^1 |S_3|^{10} \mathrm{d}\alpha_1 \mathrm{d}\alpha_3 \ll P^3 \int_0^1 \int_0^1 |S_3|^6 \mathrm{d}\alpha_1 \mathrm{d}\alpha_3 + PR, \tag{1}$$

此处 R 是方程组

$$\begin{aligned} y_1 y_2 \Delta^2 x_3^3 &= z_1^3 + z_2^3 + z_3^3 - z_4^3 - z_5^3 - z_6^3, \\ 0 &= z_1 + z_2 + z_3 - z_4 - z_5 - z_6, \quad z \ll P \end{aligned}$$

的解数. 由引理 1.2 可知

$$R \ll \sum_{z_1}^{P} \cdots \sum_{z_5}^{P} d^3(z_1^3 + \cdots - z_5^3 - (z_1 + \cdots - z_5)^3) \ll P^{5+\varepsilon}.$$

由引理 5.2 及 (1) 可知

$$\int_0^1 \int_0^1 |S_3|^{10} \mathrm{d}\alpha_1 \mathrm{d}\alpha_3 \ll P^{6+\varepsilon}. \tag{2}$$

B_3 的证明. 由引理 5.6,

$$|C_3|^4 \ll P^3 + P \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{x_3}^{P}{}^{*} e(y_1 y_2 \Delta^2(x_3^3 \alpha_3 + x_3^2 \alpha_2 + x_3 \alpha_1)) \tag{3}$$

乘以 $|C_3|^8$, 再对 $\alpha_1, \alpha_2, \alpha_3$ 各由 0 到 1 求积分, 由引理 5.4 可得

$$\int_0^1 \int_0^1 \int_0^1 |C_3|^{12} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_3 \ll P^{7+\varepsilon} + PR,$$

此处 R 乃方程组

$$\begin{aligned} y_1 y_2 w &= z_1^3 + \cdots - z_8^3, \\ 2 y_1 y_2 &= z_1^2 + \cdots - z_8^2, \\ 0 &= z_1 + \cdots - z_8, \quad z_v \ll P \end{aligned}$$

的解数. $w = \Delta^2 x_3^3 \ll P$.

由引理 5.2, 对固定的 w, 方程组

$$\begin{gathered} 2z_1^3 - w z_1^2 + \cdots - (2z_8^3 - w z_8^2) = 0, \\ z_1 + \cdots - z_8 = 0 \end{gathered}$$

的解数 $\ll P^{5+\varepsilon}$. 而对已知的 $z_1, \cdots, z_8$, 整数 y_1 及 y_2 的对数 $\leqslant d(z_1^2 + \cdots - z_8^2) = O(P^\varepsilon)$. 故得

$$R \ll \sum_w P^{5+\varepsilon} \ll P^{6+\varepsilon}.$$

因此得出

$$\int_0^1 \int_0^1 \int_0^1 |C_3|^{12} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_3 \ll P^{7+\varepsilon}. \tag{4}$$

以 $|C_3|^{12}$ 乘 (3) 式, 再由 (2) 及 (4) 式可以求出

$$\int_0^1 \int_0^1 \int_0^1 |C_3|^{16} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_3 \ll P^{10+\varepsilon}.$$

A_4 的证明. 由引理 5.6 可得

$$|S_4|^8 \ll P^7 + P^4 \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{x_3}^{P} \sum_{x_4}^{P}{}^* e(y_1 y_2 y_3 \Delta^3 (x_4^4 \alpha_4 + x_4^2 \alpha_2 + x_4 \alpha_1)).$$

乘以 $|S_4|^8$ 再求积分, 由引理 5.2 可知

$$\int_0^1 \int_0^1 \int_0^1 |S_4|^{16} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_4 \ll P^{11+\varepsilon} + P^4 R,$$

此处 R 乃方程组

$$\begin{aligned} y_1 y_2 y_3 \Delta^3 x_4^4 &= z_1^4 + \cdots - z_8^4, \\ 0 &= z_1^2 + \cdots - z_8^2, \\ 0 &= z_1 + \cdots - z_8, \quad z \ll P \end{aligned}$$

的解数.

依照定理 B_2, 由最后二式可知 $z_1, \cdots, z_8$ 的组数是 $\ll P^{8-3+\varepsilon}$. 对固定的 $z_1, \cdots, z_8$, 由第一式可知 y_1, y_2, y_3, x_4 的组数是 $\leqslant d^3(z_1^4 + \cdots - z_8^4) = O(P^\varepsilon)$. 因之 $R \ll P^{8-3+\varepsilon} = P^{5+\varepsilon}$, 故

$$\int_0^1 \int_0^1 \int_0^1 |S_4|^{16} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_4 \ll P^{11+\varepsilon}. \tag{5}$$

重复此种步骤, 可得

$$\int_0^1 \int_0^1 \int_0^1 |S_4|^{24} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_4 \ll P^{18+\varepsilon} \tag{6}$$

及

$$\int_0^1 \int_0^1 \int_0^1 |S_4|^{32} \mathrm{d}\alpha_1 \mathrm{d}\alpha_2 \mathrm{d}\alpha_4 \ll P^{25+\varepsilon}. \tag{7}$$

B_4 的证明. 由引理 5.4 显然有

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{10}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_3\mathrm{d}\alpha_4 \ll P^{5+\varepsilon}.$$

由引理 5.6,

$$|C_4|^4 \ll P^3 + P\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{x_3}^{P}{}^{*} e(y_1y_2\Delta^2(x_3^4\alpha_4 + x_3^3\alpha_3 + x_3^2\alpha_2 + x_3\alpha_1))$$

乘以 $|C_4|^{10}$ 并积分之, 可得

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{14}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_3\mathrm{d}\alpha_4 \ll P^{8+\varepsilon} + PR,$$

此处 R 乃方程组

$$\begin{aligned} y_1y_2\Delta^2x_3^4 &= z_1^4 + \cdots - z_{10}^4,\\ y_1y_2\Delta^2x_3^3 &= z_1^3 + \cdots - z_{10}^3,\\ 2y_1y_2 &= z_1^2 + \cdots - z_{10}^2,\\ 0 &= z_1 + \cdots - z_{10} \end{aligned}$$

的解数. 命 $\Delta^2x_3^3 = 2w$(易见 w 乃 y_1, y_2 及 x_3 的一次式, 其系数是整数). 对固定的 w, 由 (2) 可知方程组

$$\begin{aligned} 0 &= z_1^3 - wz_1^2 + \cdots - (x_{10}^3 - wz_{10}),\\ 0 &= z_1 + \cdots - z_{10} \end{aligned}$$

的解数是 $\ll P^{6+\varepsilon}$. 因此得出 $R \ll P^{7+\varepsilon}$. 故

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{14}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_3\mathrm{d}\alpha_4 \ll P^{8+\varepsilon}. \tag{8}$$

由引理 5.6, 可得

$$|C_4|^8 \ll P^7 + P^4\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{y_3}^{P}\sum_{x_4}^{P}{}^{*} e(y_1y_2y_3\Delta^3(x_4^4\alpha_4 + x_4^3\alpha_3 + x_4^2\alpha_2 + x_4\alpha_1)). \tag{9}$$

乘以 $|C_4|^{14}$ 且积分之, 可得

$$\int_0^1\int_0^1\int_0^1\int_0^1 |C_4|^{22}\mathrm{d}\alpha_1\mathrm{d}\alpha_2\mathrm{d}\alpha_3\mathrm{d}\alpha_4 \ll P^{15+\varepsilon} + P^4R,$$

此处 R 乃方程组

$$\begin{aligned}6y_1y_2y_3w&=z_1^4+\cdots-z_{14}^4,\\6y_1y_2y_3&=z_1^3+\cdots-z_{14}^3,\\0&=z_1^2+\cdots-z_{14}^2,\\0&=z_1+\cdots-z_{14},\end{aligned}$$

的解数, 此处 $w=\dfrac{1}{6}\Delta^3x_4^4$ 乃 y_1,y_2,y_3 及 x_4 的一次式, 其系数是整数. 易见, R 不超过方程组

$$\begin{aligned}z_1^4-wz_1^3+\cdots-(z_{14}^4-wz_{14}^3)=0,\\z_1^2+\cdots-z_{14}^2=0,\\z_1+\cdots-z_{14}=0\end{aligned}$$

的解数的 $\ll P^{1+\varepsilon}$ 倍. 由引理 5.2 可知

$$R\ll P^{1+\varepsilon}P^{14-4+\varepsilon}\ll P^{11+\varepsilon}$$

及

$$\int_0^1\int_0^1\int_0^1\int_0^1|C_4|^{22}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_4\ll P^{15+\varepsilon}.\tag{10}$$

如法进行但由 (5), (6) 代替引理 5.2 我们得出

$$\int_0^1\int_0^1\int_0^1\int_0^1|C_4|^{22+8\lambda}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_4\ll P^{15+7\lambda+\varepsilon},\quad\lambda=1,2,3.\tag{11}$$

今后将用简写法

$$\int f\mathrm{d}x$$

代替

$$\int_0^1\int_0^1\cdots\int_0^1 f(x_1,\cdots x_n)\mathrm{d}x_1\mathrm{d}x_2\cdots\mathrm{d}x_n.$$

A_5 的证明. 由引理 5.6,

$$|S_5|^4\ll P^3+P\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{x_3}^{P}e(y_1y_2\Delta^2g(x_3)),$$

此处 $g(x_3)=x_3^5\alpha_5+x_3^3\alpha_3+x_3^2\alpha_2+x_3\alpha_1$. 乘以 $|S_5|^{10}$ 且积分, 可得

$$\int|S_5|^{14}\mathrm{d}\alpha\ll P^{8+\varepsilon}+PR,$$

此处 R 乃方程组*

$$\begin{aligned} y_1y_2\Delta^2x_3^5 &= z_1^5+\cdots-z_{10}^5,\\ 2y_1y_2w &= z_1^3+\cdots-z_{10}^3,\\ 2y_1y_2 &= z_1^2+\cdots-z_{10}^2,\\ 0 &= z_1+\cdots-z_{10} \end{aligned}$$

的解数. 对固定的 w, 由 A_3 可知

$$\begin{aligned} z_1^3-wz_1^2+\cdots-(z_{10}^3-wz_{10}^2) &= 0,\\ z_1+\cdots-z_{10} &= 0 \end{aligned}$$

的解数 $\ll P^{6+\varepsilon}$. 故得出 $R\ll P^{7+\varepsilon}$. 即得

$$\int|S_5|^{14}\mathrm{d}\alpha\ll P^{8+\varepsilon}. \tag{12}$$

由引理 5.6,

$$|S_5|^8\ll P^7+P^4\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{y_3}^{P}\sum_{x_4}^{P}{}^{*}e(y_1y_2y_3\Delta^3g(x_4)).$$

乘以 $|S_5|^{14}$ 且积分, 得

$$\int|S_5|^{22}\mathrm{d}\alpha\ll P^{15+\varepsilon}+P^4R,$$

此 R 乃方程组

$$\begin{aligned} y_1y_2y_3\Delta^3x_3^5 &= z_1^5+\cdots-z_{14}^5,\\ 6y_1y_2y_3 &= z_1^3+\cdots-z_{14}^3,\\ 0 &= z_1^2+\cdots-z_{14}^2,\\ 0 &= z_1+\cdots-z_{14} \end{aligned}$$

的解数.

故由 B_2 可知, $R\ll P^{14-3+\varepsilon}$. 由此得出

$$\int|S_5|^{22}\mathrm{d}\alpha\ll P^{15+\varepsilon}.$$

* 今后不再重复 w 的定义.

由引理 5.6,

$$|S_5|^{16} \ll P^{15} + P^{11} \sum_{y_1}^{P} \sum_{y_2}^{P} \sum_{y_3}^{P} \sum_{y_4}^{P} \sum_{x_5}^{P}{}^{*} e(y_1 y_2 y_3 y_4 \Delta^4 g(x_5)).$$

乘以 $|S_5|^{22}$ 且积分, 由 B_3 可得

$$\int |S_5|^{38} \mathrm{d}\alpha \ll P^{30+\varepsilon}. \tag{13}$$

重复此一手续, 可得

$$\int |S_5|^{38+16\lambda} \mathrm{d}\alpha \ll P^{30+15\lambda+\varepsilon}, \quad \lambda = 1, 2, 3. \tag{14}$$

§5.6 定理的证明 (续)

当 $k \geqslant 5$ 时, 命 $l \geqslant 1, a = \dfrac{1}{k}$ 及

$$u = \frac{1}{4}k(k+1) + \begin{cases} 0, & \text{当 } k \equiv 0, 3 \pmod 4, \\ \dfrac{1}{2}, & \text{当 } k \equiv 1, 2 \pmod 4). \end{cases} \tag{1}$$

在引理 4.7 中取 $u_0 = k+1$. 由引理 5.4 可知对任一 $\varepsilon > 0$ 此引理之假定当 $v_0 = k+1+\varepsilon$ 时真实. 因此得出

$$\int |C_k(P)|^{2u} \mathrm{d}\alpha \leqslant b(k, \varepsilon) P^{2u - \frac{1}{2}k(k+1) + \delta + \varepsilon}, \tag{2}$$

此处

$$\delta = \frac{k^2(k^2 - k - 2)}{2(u + k^2 - k - 1)}. \tag{3}$$

用引理 4.4 l 次得到

$$\begin{aligned} &\int |C_k(P)|^{2(u+lk)} \mathrm{d}\alpha \\ \ll & P^{2kl - \frac{1}{2}k(k+1) + \frac{1}{2}k(k+1)(1-a)^l + 2u(1-(1-a)^l) + \varepsilon} \\ & \times \int |C_k(P^{(1-a)^l})|^{2u} \mathrm{d}\alpha \ll P^{2(u+lk) - \frac{1}{2}k(k+1) + \delta(1-a)^l + \varepsilon}. \end{aligned} \tag{4}$$

今当 $5 \leqslant k \leqslant 10$ 时, 分别取 l 的值如下表, 并算出其相应的 $\delta(1-a)^l$ 及 $2(u+lk)$ 的数值:

k	5	6	7	8	9	10
u	8	11	14	18	23	28
l	5	10	16	23	29	34
$\delta(1-a)^l <$	2.74	2.04	1.52	1.098	0.991	1.046
$2(u+lk)$	66	142	252	404	568	736

B_5 的证明: 由 (4) 式及上表, 可得

$$\int |C_5|^{66}\mathrm{d}\alpha \ll P^{66-15+2.74+\varepsilon}. \tag{5}$$

由引理 5.6,

$$|C_5|^{16} \ll P^{15} + P^{11}\sum_{y_1}^{P}\sum_{y_2}^{P}\sum_{y_3}^{P}\sum_{y_4}^{P}\sum_{x_5}^{P}{}^{*}e(y_1y_2y_3y_4\Delta^4 g(x_5)), \tag{6}$$

此式两端乘以 $|C_5|^{66}$ 并积分之, 可得

$$\int |C_5|^{82}\mathrm{d}\alpha \ll P^{82-15+1.74+\varepsilon} + P^{12+\varepsilon}\int |S_5|^{66}\mathrm{d}\alpha. \tag{7}$$

由 B_5 及凸函数的性质, 易知

$$\int |S_5|^{66}\mathrm{d}\alpha \ll P^{45+12\times\frac{15}{16}+\varepsilon} = P^{56.25+\varepsilon}.$$

故由 (7) 即得

$$\int |C_5|^{82}\mathrm{d}\alpha \ll P^{82-15+1.74+\varepsilon}. \tag{8}$$

由 (5) 和 (8), 可得

$$\int |C_5|^{78}\mathrm{d}\alpha \ll P^{78-15+1.99+\varepsilon}. \tag{9}$$

重复上述手续, 可得

$$\int |C_5|^{110}\mathrm{d}\alpha \ll P^{95+\varepsilon}. \tag{10}$$

A_6 和 B_6 的证明: 由 (4) 式及上表, 可得

$$\int |C_6|^{142}\mathrm{d}\alpha \ll P^{142-21+2.04+\varepsilon}. \tag{11}$$

由引理 5.5 可得

$$\int |S_6|^{142}\mathrm{d}\alpha \ll P^{142-16+2.04+\varepsilon}. \tag{12}$$

应用引理 5.6 中 $\mu=5$ 的情况, 并用 B_4, 可得

$$\int |S_6|^{142+32\lambda}\mathrm{d}\alpha \ll P^{142+32\lambda-16+(2.04-2\lambda)+\varepsilon}, \quad \lambda=1,2. \tag{13}$$

由 (13) 可得

$$\int |S_6|^{176}\mathrm{d}\alpha \ll P^{176-16+0.98+\varepsilon}. \tag{14}$$

再应用引理 5.6 中 $\mu=5$ 的情况, 并用 B_4 即可得

$$\int |S_6|^{208}\mathrm{d}\alpha \ll P^{208-16+\varepsilon}. \tag{15}$$

由 (11) 直接得出

$$\int |C_6|^{174}\mathrm{d}\alpha \ll P^{155.04+\varepsilon}. \tag{16}$$

再利用上式, 并应用引理 5.6 中 $\mu=5$ 的情况及 (13) 可得

$$\int |C_6|^{206}\mathrm{d}\alpha \ll P^{186.04+\varepsilon}. \tag{17}$$

由 (16), (17) 可以得到

$$\int |C_6|^{176}\mathrm{d}\alpha \ll P^{156.98}. \tag{18}$$

再重复上面的步骤, 可得

$$\int |C_6|^{208}\mathrm{d}\alpha \ll P^{187.98+\varepsilon}. \tag{19}$$

$$\int |C_6|^{240}\mathrm{d}\alpha \ll P^{219+\varepsilon}. \tag{20}$$

A_7 和 B_7 的证明：由 (4) 式及所列的表, 可得

$$\int |C_7|^{252}\mathrm{d}\alpha \ll P^{224+1.52+\varepsilon}. \tag{21}$$

由引理 5.5,

$$\int |S_7|^{252}\mathrm{d}\alpha \ll P^{230+1.52+\varepsilon}. \tag{22}$$

应用引理 5.6 中 $\mu=6$ 的情况, 并用 B_5, 可得

$$\int |S_7|^{316}\mathrm{d}\alpha \ll P^{294+0.52+\varepsilon}. \tag{23}$$

由 (22) 和 (23) 可得

$$\int |S_7|^{286}\mathrm{d}\alpha \ll P^{264+0.99+\varepsilon}. \tag{24}$$

再应用引理 5.6 中 $\mu=6$ 的情况, 并且 B_5, 即得出

$$\int |S_7|^{350}\mathrm{d}\alpha \ll P^{328+\varepsilon}. \tag{25}$$

由 (21) 直接得出

$$\int |C_7|^{316}\mathrm{d}\alpha \ll P^{288+1.52+\varepsilon}. \tag{26}$$

应用引理 5.6 中 $\mu=6$ 的情况及 (23), 可得

$$\int |C_7|^{380}\mathrm{d}\alpha \ll P^{352+0.52+\varepsilon}. \tag{27}$$

由 (26) 和 (27) 得出

$$\int |C_7|^{350}\mathrm{d}\alpha \ll P^{322+0.99+\varepsilon}. \tag{28}$$

应用引理 5.6 中 $\mu=6$ 的情况及 B_7 即得

$$\int |C_7|^{414}\mathrm{d}\alpha \ll P^{386+\varepsilon}. \tag{29}$$

A_8 和 B_8：由 (4) 及上表可得

$$\int |C_8|^{404}\mathrm{d}\alpha \ll P^{368+1.098+\varepsilon}, \tag{30}$$

$$\int |C_8|^{420}\mathrm{d}\alpha \ll P^{384+1.098\times\frac{7}{8}+\varepsilon} \ll P^{384+0.962+\varepsilon}. \tag{31}$$

由此两式可得

$$\int |C_8|^{416}\mathrm{d}\alpha \ll P^{380+0.996+\varepsilon}. \tag{32}$$

与 A_7, B_7 的证明相似, 由 (32) 可得

$$\int |S_8|^{544}\mathrm{d}\alpha \ll P^{515+\varepsilon}. \tag{33}$$

$$\int |C_8|^{672}\mathrm{d}\alpha \ll P^{636+\varepsilon}. \tag{34}$$

与 A_8, B_8 完全类似, 我们可以得出如下的结果:

A_9 :

$$\int |S_9|^{824}\mathrm{d}\alpha \ll P^{787+\varepsilon}. \tag{35}$$

B_9 : $$\int |C_9|^{1080}\mathrm{d}\alpha \ll P^{1035+\varepsilon}. \tag{36}$$

A_{10}: $$\int |S_{10}|^{1258}\mathrm{d}\alpha \ll P^{1212+\varepsilon}. \tag{37}$$

B_{10}: $$\int |C_{10}|^{1770}\mathrm{d}\alpha \ll P^{1715+\varepsilon}. \tag{38}$$

§5.7 单和与平均值之间的关系

引理 5.7 命 $\tau \geqslant 1$ 及

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{\tau}{q^2}, \quad (h,q)=1,$$

则适合不等式

$$\{\alpha y\} \leqslant \frac{V}{q}, \quad f \leqslant y \leqslant f+N$$

的整数 y 的个数

$$\leqslant 2(V+2\tau)\left(\frac{N}{q}+1\right).$$

证 若能证明适合

$$\{\alpha y\} \leqslant \frac{V}{q}, \quad f \leqslant y \leqslant f+q \tag{1}$$

的整数 y 的个数 $\leqslant 2(V+2\tau)$, 则本引理即已证明. 今写

$$y=f+z, \quad \alpha = \frac{h}{q}+\frac{\tau\vartheta}{q^2}, \quad |\vartheta| \leqslant 1,$$

则

$$\begin{aligned}\alpha y &= \frac{hz}{q}+\frac{\tau\vartheta z}{q^2}+\frac{hf}{q}+\frac{\tau\vartheta f}{q^2}\\ &= \frac{hz+[c]+(c-[c])+\tau\vartheta z/q}{q}, \quad \left|\frac{\tau\vartheta z}{q}\right| \leqslant \tau,\end{aligned}$$

此处 $c=hf+\tau\vartheta f/q$.

如果 $q \leqslant 2(V+2\tau)$, 定理显然真实. 当 z 经过一完全剩余系, mod q, 则 $w=hz+[c]$ 也是如此. 所以

$$\alpha y = \frac{w+\sigma(w)}{q},$$

此处

$$-\tau \leqslant c-[c]-\tau \leqslant \sigma(w) \leqslant c-[c]+\tau < 1+\tau.$$

适合不等式

$$V+\tau \leqslant w < q-\tau-V-1 \tag{2}$$

的 w 显然也适合不等式

$$\frac{V}{q} \leqslant \frac{w+\sigma(w)}{q} < 1-\frac{V}{q}.$$

而这并不适合 (1) 式. 适合 (2) 的整数 w 的个数 $\geqslant q-2V-2\tau-2$, 所以适合 (1) 的整数的个数

$$\leqslant q-(q-2V-2\tau-2)=2V+2\tau+2\leqslant 2(V+2\tau).$$

引理 5.8　命 $Y\geqslant 1$. 又命 $A_0, A_1, \cdots, A_{k-1}$ 是适合

$$A_0=1,\quad |A_r|\leqslant (r+1)Y^r$$

的整数. 则由方程组

$$v_r=\sum_{s=r}^{k}\binom{s+1}{r}A_{s-r}u_s \tag{3}$$

可以解得 $(k+1)k\cdots(r+1)u_r$ 是 $v_1, \cdots, v_r$ 的线性式, 其系数都是整数, 即

$$(k+1)k\cdots(r+1)u_r=\sum_{s=r}^{k}a_{rs}v_s \tag{4}$$

且

$$a_{rs}=O(Y^{s-r}).$$

证　当 $r=k$ 时, 这引理显然真实. 假定对 $k, k-1, \cdots, r+1$ 时, 这引理都真实. 由 (3) 式可知

$$\begin{aligned}
&(k+1)\cdots(r+1)u_r\\
&=(k+1)\cdots(r+2)\left(v_r-\sum_{s=r+1}^{k}\binom{s+1}{r}A_{s-r}u_s\right)\\
&=(k+1)\cdots(r+2)v_r-\sum_{s=r+1}^{k}\binom{s+1}{r}A_{s-r}\frac{s!}{(r+1)!}(k+1)\cdots(s+1)u_s\\
&=(k+1)\cdots(r+2)v_r-\sum_{s=r+1}^{k}\binom{s+1}{r}A_{s-r}\frac{s!}{(r+1)!}\sum_{s\leqslant u\leqslant k}\alpha_{su}v_u.
\end{aligned}$$

当 $k\geqslant u>r$ 时,

$$a_{ru}=\sum_{r+1\leqslant s\leqslant u}\binom{s+1}{r}A_{s-r}\frac{s!}{(r+1)!}\alpha_{su}$$

显然是一整数, 且

$$a_{ru}=O\left(\sum_{r+1\leqslant s\leqslant u}|A_{s-r}|\,|a_{su}|\right)$$
$$=O(Y^{s-r}\cdot Y^{u-s})=O(Y^{u-r}).$$

当 $u=r$ 时, 显然

$$a_{rr}=O(1).$$

引理 5.9 命 $\xi_1,\cdots,\xi_n$ 表实数. 则对整数 $l_1,\cdots,l_n$ 我们有不等式

$$\left\{\sum_{i=1}^{n}l_i\xi_i\right\}\leqslant\sum_{i=1}^{n}|l_i|\{\xi_i\}.$$

这引理是下面不等式的推理:

$$\{\xi_1\pm\xi_2\}\leqslant\{\xi_1\}+\{\xi_2\}.$$

引理 5.10 命 $\alpha_k,\cdots,\alpha_1$, 是实数,

$$f(x)=\alpha_kx^k+\cdots+\alpha_1x.$$

假定我们有以下的事实: 命 $0<\delta_1<1,T$ 是任意整数, 则

$$\int_0^1\cdots\int_0^1\left|\sum_{x=T+1}^{T+P}e(f(x))\right|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k=O(P^{2t_1-\frac{1}{2}k(k+1)+\delta_1}),\tag{5}$$

此处符号 O 所包含的常数依于 t_1,δ_1 及 k, 但将来事实上 t_1,δ_1 都是 k 的函数. 在这样的假定下我们有:

命 $\beta_{k+1},\cdots,\beta_1$ 表实数,

$$F(x)=\beta_{k+1}x^{k+1}+\cdots+\beta_1x.$$

又命 r 是适合于 $2\leqslant r\leqslant k+1$ 的整数. 假定

$$\left|\beta_r-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\quad(h,q)=1,\ 1\leqslant q\leqslant P^r,\tag{6}$$

则对任一 $T=O(P)$, 我们有

$$S=\sum_{x=T+1}^{T+P}e(F(x))=O\begin{cases}P^{1-\rho}\left(\dfrac{P}{q}\right)^{\frac{1}{2t_1+k+1}}, & \text{当 } 1\leqslant q\leqslant P,\\ P^{1-\rho}, & \text{当 } P\leqslant q\leqslant P^{r-1},\\ P^{1-\rho}\left(\dfrac{q}{P^{r-1}}\right)^{\frac{1}{2t_1+k+1}}, & \text{当 } P^{r-1}\leqslant q\leqslant P^r,\end{cases}$$

此处

$$\rho=\frac{1-\delta_1}{2t_1+k+1}.$$

证　(这一重要技巧是Виноградов所发明的).　当 $0<y\leqslant Y<P$ 时, 命

$$S_0=\sum_{x=T+1}^{T+P}e(F(x+y)-F(y))=\sum_{x=T+1}^{T+P}e(\phi(x)),$$

此处

$$\begin{aligned}\phi(x)&=Y_1x+\cdots+Y_{k+1}x^{k+1},\\ Y_j&=Y_j(y)=\frac{1}{j!}\frac{d^j}{dy^j}F(y)\\ &=\binom{k+1}{j}\beta_{k+1}y^{k+1-j}+\cdots+\binom{j+1}{j}\beta_{j+1}y+\beta_j.\end{aligned}\tag{7}$$

显然有

$$|S_0|=|S|+2\vartheta y,\quad |\vartheta|\leqslant 1.$$

因此

$$|S|=O\left(Y^{-1}\sum_{y=1}^{Y}|S_0|+Y\right).$$

用 Hölder 不等式两次, 有

$$|S|^{2t_1}=O\left(\left(Y^{-1}\sum_{y=1}^{Y}|S_0|\right)^{2t_1}+Y^{2t_1}\right)=O\left(Y^{-1}\sum_{y=1}^{Y}|S_0|^{2t_1}+Y^{2t_1}\right).\tag{8}$$

命

$$S_1=\sum_{x=T+1}^{T+P}e(\alpha_1x+\cdots+\alpha_kx^k+\beta_{k+1}x^{k+1}).$$

对一固定的 $y,Y_1,\cdots,Y_k$ 也定. 今讨论适合于

$$\{\alpha_1-Y_1\}\leqslant\frac{1}{2}P^{-2}Y,\cdots,\{\alpha_k-Y_k\}\leqslant\frac{1}{2}P^{-k-1}Y,\quad 0\leqslant\alpha_i<1$$

的实数组 $\alpha_1,\cdots,\alpha_k$. 如此所得出的 $(\alpha_1,\cdots,\alpha_k)$ 所成之域, 用 $Q(y)$ 表它. 如果 $(\alpha_1,\cdots,\alpha_k)$ 在 $Q(y)$ 中, 则

$$S_0=S_1+O(Y),$$

即得

$$|S_0|^{2t_1}=O(|S_1|^{2t_1})+O(Y^{2t_1}).$$

积分等式两边, 其积分区域是 $Q(y)$, 则得

$$|S_0|^{2t_1} = O\left(P^{\frac{1}{2}k(k+1)+k}Y^{-k}\int\underset{Q(y)}{\cdots}\int|S_1|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right)+O(Y^{2t_1}), \tag{9}$$

此处用上了

$$\int\underset{Q(y)}{\cdots}\int\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k \gg \prod_{i=1}^{k}(P^{-(i+1)}Y) = P^{-\frac{1}{2}k(k+1)-k}Y^k.$$

联合 (8) 及 (9) 可知

$$|S|^{2t_1} = O\left(P^{\frac{1}{2}k(k+1)+k}Y^{-k-1}\sum_{y=1}^{Y}\int\underset{Q(y)}{\cdots}\int|S_1|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right)+O(Y^{2t_1}). \tag{10}$$

今往计算: 有多少个不同的 y, 使 $Q(y)$ 皆包有一固定的点. 若 $Q(y)$ 及 $Q(y_0)$ 有一公共点, 则

$$\{Y_r(y)-Y_r(y_0)\} \leqslant P^{-r-1}Y, \quad 1\leqslant r\leqslant k.$$

命 $v_r = Y_r(y)-Y_r(y_0), u_s = \beta_{s+1}(y-y_0)$ 及

$$A_{s-r} = \frac{y^{s-r+1}-y_0^{s-r+1}}{y-y_0}.$$

由 (7) 可知

$$\begin{aligned} v_r &= \sum_{r\leqslant s\leqslant k}\binom{s+1}{r}\beta_{s+1}(y^{s-r+1}-y_0^{s-r+1}) \\ &= \sum_{r\leqslant s\leqslant k}\binom{s+1}{r}A_{s-r}u_s. \end{aligned}$$

由引理 5.8 及 5.9 可知, 当 $1\leqslant r<k$ 时

$$\begin{aligned} \left\{\frac{(k+1)!}{r!}u_r\right\} &\leqslant \sum_{r\leqslant s\leqslant k}|a_{rs}|\{v_s\} \\ &= O\left(\sum_{r\leqslant s\leqslant k}Y^{s-r}P^{-s-1}Y\right) \\ &= O(YP^{-r-1}). \end{aligned}$$

以 r 代 $r-1$, 则得, 当 $2 \leqslant r < k+1$ 时

$$\left\{\frac{(k+1)!}{(r-1)!}\beta_r(y-y_0)\right\} = O(YP^{-r}), \tag{11}$$

此处

$$1 \leqslant y \leqslant Y. \tag{12}$$

由引理 5.7, 可知适合 (11) 及 (12) 的 y 的个数是

$$O\left(\left(\frac{Yq}{P^r}+1\right)\left(1+\frac{Y}{q}\right)\right) = O\left(1+\frac{Y}{q}+\frac{Yq}{P^r}\right).$$

(因为 $Y^2 \leqslant P^2 \leqslant P^r$).

故 k 维单位方体

$$0 \leqslant \alpha_1 \leqslant 1, \cdots, \quad 0 \leqslant \alpha_k \leqslant 1$$

中每一点 $(\alpha_1, \cdots, \alpha_k)$ 最多为 $O\left(1+\frac{Y}{q}+\frac{Yq}{P^r}\right)$ 个 $Q(y)(y=1,\cdots,Y)$ 所盖上. 所以由 (10) 可知

$$\begin{aligned}|S|^{2t_1} =& O\left(P^{\frac{1}{2}k(k+1)+k}Y^{-k-1}\left(1+\frac{Y}{q}+\frac{Yq}{P^r}\right)\int_0^1\cdots\int_0^1 |S_1|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right) \\ &+ O(Y^{2t_1}).\end{aligned}$$

由

$$\int_0^1\cdots\int_0^1 |S_1|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k \leqslant \int_0^1\cdots\int_0^1\left|\sum_{x=T+1}^{T+P} e(f(x))\right|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k$$

及 (5) 式可知

$$\begin{aligned}|S|^{2t_1} &= O\left(P^{\frac{1}{2}k(k+1)+k}Y^{-k-1}\left(1+\frac{Y}{q}+\frac{Yq}{P^r}\right)P^{2t_1-\frac{1}{2}k(k+1)+\delta_1}\right)+O(Y^{2t_1}) \\ &= O\left(P^{2t_1+k+\delta_1}Y^{-k-1}\left(1+\frac{Y}{q}+\frac{Yq}{P^r}\right)\right)+O(Y^{2t_1}).\end{aligned}$$

取

$$Y = \begin{cases}\left[P^{1-\rho}\left(\frac{P}{q}\right)^{\frac{1}{2t_1+k+1}}\right]+1, & \text{当 } P^{\delta_1} \leqslant q \leqslant P, \\ [P^{1-\rho}]+1, & \text{当 } P \leqslant q \leqslant P^{r-1}, \\ \left[P^{1-\rho}\left(\frac{q}{P^{r-1}}\right)^{\frac{1}{2t_1+k+1}}\right]+1, & \text{当 } P^{r-1} \leqslant q \leqslant P^{r-\delta_1},\end{cases}$$

即得出引理.

§5.8　三角和的估值

定理 9　用下面的表来定义 σ_k 的数值：

k	2	3	4	5	6	7	8	9	10	11	$\geqslant 12$
σ_k	4	9	20	51	116	247	422	681	1090	1781	$2k^2\ (2\log k + \log\log k + 3)$

命 $2 \leqslant r \leqslant k$,

$$\left|\alpha_r - \frac{h}{q}\right| \leqslant \frac{1}{q^2}, \quad (h,q)=1,\ 1 \leqslant q \leqslant P^r, \tag{1}$$

又命

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x,$$

则当 $P \leqslant q \leqslant P^{r-1}$ 时,

$$\sum_{x=1}^{P} e(f(x)) = O\left(P^{1-\frac{1}{\sigma_k}+\varepsilon}\right). \tag{2}$$

证　当 $k \leqslant 11$, 这结果可由引理 5.10(其中 $\delta_1 = \varepsilon, \sigma_k = 2t_1 + k$) 及定理 7 直接推出.

当 $k > 11$ 时, 在定理 5 中, 取

$$l = \left[\frac{2\log k + \log\log k}{-\log\left(1-\dfrac{1}{k}\right)}\right] + 1,$$

此时

$$t_1 = \frac{1}{4}k(k-1) + l(k-1) + \begin{cases} 0, & 若\ k \equiv 0,3 \pmod 4, \\ \dfrac{1}{2} & 若\ k \equiv 1,2 \pmod 4, \end{cases}$$

$$\delta_1 = \frac{1}{2}k(k-1)\left(1-\frac{1}{k-1}\right)^l.$$

由于

$$k-1 \leqslant \frac{1}{-\log\left(1-\dfrac{1}{k}\right)} = \left(\frac{1}{k} + \frac{1}{2k^2} + \frac{1}{3k^3} + \cdots\right)^{-1} \leqslant k.$$

易得

$$\frac{1}{2}(k+1) < l < k(2\log k + \log\log k) + 1,$$

$$\delta_1 < \frac{1}{2}k^2\left(1-\frac{1}{k}\right)^l \leqslant \frac{1}{2\log k} < \frac{1}{2}.$$

因为对于适合 $0 \leqslant x \leqslant \frac{1}{2}$ 的 x, 常有

$$(1-x)^{-1} \leqslant 1 + 2x,$$

所以得到

$$\begin{aligned}\frac{1}{\rho} &= \frac{2t_1+k}{1-\delta_1} \leqslant \left(\frac{1}{2}k^2 + 2l(k-1) + k + 1\right)(1+2\delta_1)\\ &\leqslant \left\{\frac{1}{2}k^2 + 2k(2k\log k + k\log\log k + 1)\right\}\left(1+\frac{1}{\log k}\right)\\ &\leqslant 2k^2\left(2\log k + \log\log k + 2 + \frac{1}{4} + \frac{\log\log k}{\log k} + \frac{1}{4\log k} + \frac{1}{k} + \frac{1}{k\log k}\right)\\ &\leqslant 2k^2(2\log k + \log\log k + 3).\end{aligned}\tag{3}$$

于是由定理 5 及引理 5.10 得到定理.

定理 7 及引理 5.10 的另一推理如次:

引理 5.11　设 $k \leqslant 11$, 则在定理 9 的条件下, 有

$$\sum_{x=1}^{P} \mathrm{e}^{\pi i f(x)} \ll \begin{cases} P^{1-\frac{1}{\sigma_k}+\varepsilon}\left(\dfrac{P}{q}\right)^{\frac{1}{\sigma_k}}, & \text{当 } 1 \leqslant q \leqslant P,\\ P^{1-\frac{1}{\sigma_k}+\varepsilon}\left(\dfrac{q}{P^{r-1}}\right)^{\frac{1}{\sigma_k}}, & \text{当 } P^{r-1} \leqslant q \leqslant P^r.\end{cases}$$

当 $k \geqslant 12$ 时, 目前我们不能获得如此精确的结果. 但为了以后的应用, 我们先给予如下的初步结果:

引理 5.12　设 $k \geqslant 12$, 则在定理 9 的条件下, 当 $P^{1/(4k)} \leqslant q \leqslant P$ 及 $P^{r-1} \leqslant q \leqslant P^{r-1/(4k)}$ 时, 有

$$\sum_{x=1}^{P} \mathrm{e}^{2\pi i f(x)} \ll P^{1-\frac{1}{\rho'}}, \quad \rho' = 50\,k^3\log k.$$

证　由引理 5.10, 我们知道

$$\sum_{x=1}^{P} \mathrm{e}^{2\pi i f(x)} \ll P^{1-\rho}\left\{\begin{matrix} P^{\frac{1}{2t_1+k}-\frac{1}{4k(2t_1+k)}}\\ P^{\frac{1-r}{2t_1+k}+\frac{r-1/4k}{2t_1+k}}\end{matrix}\right\} \ll P^{1-\frac{1/4k-\delta_1}{2t_1+k}}.$$

此处

$$\delta_1 = \frac{1}{2}k(k-1)\left(1-\frac{1}{k-1}\right)^l.$$

取

$$l = \left[\frac{4\log k}{-\log(1-1/k)}\right]+1,$$

则

$$\frac{1}{2}(k+1) \leqslant l \leqslant 4k\log k + 1$$

及

$$\delta_1 \leqslant k^2\left(1-\frac{1}{k}\right)^l \leqslant \frac{1}{k^2}.$$

亦如证明 (3) 式, 可得

$$\begin{aligned}
&(2t_1+k+1)\Big/\left(\frac{1}{4k}-\delta_1\right)\\
\leqslant&\left(\frac{1}{2}k^2+2lk\right)\Big/\left(\frac{1}{4k}-\frac{1}{k^2}\right)\\
\leqslant&\left(\frac{1}{2}k^2+8k^2\log k+2k\right)4k\left(1-\frac{4}{k}\right)^{-1}\\
\leqslant&4k^3\log k\left(8+\frac{1}{2\log k}+\frac{2}{k\log k}\right)\left(1-\frac{4}{k}\right)^{-1}\\
\leqslant&4k^3\log k\left(8+\frac{2}{3\log 12}\right)\left(\frac{3}{2}\right)\\
<&50k^3\log k.
\end{aligned}$$

附记：较引理 5.12 更完整的结果如下：当 $k \leqslant 9$ 及 $P^{r-1} \leqslant q \leqslant P^r$ 时,

$$\sum_{x=1}^{P} \mathrm{e}^{2\pi i f(x)} \ll P^{1-1/\sigma'}\left(\frac{q}{P^{r-1}}\right)^{1/\sigma'},$$

此处

$$\sigma' = k^3(3\log k + \log\log k + 5).$$

这一结果可由以后证明的定理 16 推出之.

第 6 章　含有素数变数的三角和

§6.1

本章的目的在证明定理 10, 这是堆垒素数论的基本工具. 定理 10 基本上是И.М. Виноградов*所创造的, 今后作若干必要的扩充, 使其能够适合地用到本书所讨论的问题. 我们常以 L 代表 $\log P$.

定理 10　命 $0 < Q \leqslant c_1(k)L^{\sigma_1}$ 及

$$S = \sum_{\substack{p \leqslant P \\ p \equiv t (\bmod Q)}} e(f(p)),$$

式中

$$f(x) = \frac{h}{q}x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k, \quad (h, q) = 1,$$

而 α 是实数. 并设 $L^\sigma < q \leqslant P^k L^{-\sigma}$. 对任一 $\sigma_0 > 0$, 当 $\sigma \geqslant 2^{6k}(\sigma_0 + \sigma_1 + 1)$ 时, 常有

$$|S| \leqslant c_2(k) P L^{-\sigma_0} Q^{-1}.$$

§6.2　若干必要的引理

引理 6.1　当 $\sigma_2 \geqslant 2^{3t} - 1$ 时,

$$\sum_{0<z\leqslant M}{}' (d(z))^t = O(M(\log M)^{-\sigma_2}),$$

此处 $\sum'$ 表示一和, 其中之 z 都适合下面的不等式

$$(\log M)^{\sigma_2} \leqslant c_3(d(z))^t.$$

证　由引理 2.5, 我们得到

$$(\log M)^{2\sigma_2} \sum_{0<z\leqslant M}{}' (d(z))^t \ll \sum_{0<z\leqslant M} (d(z))^{3t}$$
$$\ll M(\log M)^{2^{3t}-1} \ll M(\log M)^{\sigma_2}.$$

---

*Трудbl МатеМатиЧеск0Г0 иНститута, ТбиПиси, III, 1937, 1—34, 35—61.

由此即得出本引理.

引理 6.2 命 l 是一正整数 ($\leqslant L^{\sigma_3}$), Q 是一 $\ll L^{\sigma_4}$ 的正整数,

$$f(x)=\frac{h}{q}x^k+\alpha_1x^{k-1}+\cdots+\alpha_k,\quad (h,q)=1,$$

此处 α 是实数, 并设 $L^\sigma<q\leqslant P^kL^{-\sigma}$. 则当

$$\sigma\geqslant 2^k(\sigma_0+\sigma_3)+2k\sigma_4+2^{3(k-2)}$$

时,

$$S=\sum_{\substack{lx\leqslant P\\ lx\equiv t(\bmod Q)}}e(f(lx))=O(P_1L^{-\sigma_0}),$$

此处 $P_1=P/Ql$.

证 如果相合式 $lx\equiv t(\bmod Q)$ 没有解答, 则本引理不证自明. 命 t' 是这相合式的最小正数解, 则其他的解可以表成 $x=t'+Q\,y/(l,Q)$ 的形式, 而 $0\leqslant y\leqslant P_2=P(Q,l)/Ql$. 所以 S 可以写成

$$S=\sum_{y\leqslant P_2}e(f(l'Qy+lt')),\quad l'=l/(Q,l).$$

若 $k=1$, 这引理可由引理 1.8 得出,

$$|S|=\sum_{x\leqslant P_2}\left|e\left(\frac{h}{q}(l'Qx+lt')\right)\right|\leqslant q\leqslant PL^{-\sigma}\ll P_1L^{-\sigma_0}.$$

假定 $k>1$. 由引理 3.3, 3.4 及 1.8 可知

$$|S|^{2^{k-1}}\ll P_2^{2^{k-1}-1}+P_2^{2^{k-1}-k}\sum_{\xi_1=1}^{P_2}\cdots\sum_{\xi_{k-1}=1}^{P_2}\min\left(P_2,\frac{1}{2\left\{l'^kQ^kk!\dfrac{h}{q}\xi_1\cdots\xi_{k-1}\right\}}\right)\quad(1)$$

或写成

$$|S|^{2^{k-1}}\ll P_2^{2^{k-1}-1}+P_2^{2^{k-1}-k}\sum,$$

此 $\sum$ 代表前式右边之和.

命

$$z=l'^kQ^kk!\xi_1\cdots\xi_{k-1},\quad(2)$$

则得 $z\leqslant l'^kQ^kk!P_2^{k-1}=M$.

对一固定的 z, (2) 式的解数 $\leqslant \mathrm{d}^{k-2}(z)$. 由引理 6.1, 当 $\sigma_2 \geqslant 2^{3(k-2)}-1$ 时

$$\sum \ll P_2 \sum_{z=1}^{M}{}' d^{k-2}(z) + L^{\sigma_2}\sum_{z=1}^{M}\min\left(P_2, \frac{1}{2\{hz/q\}}\right)$$
$$\ll ML^{-\sigma_2}P_2 + L^{\sigma_2}\sum_{z=1}^{M}\min\left(P_2, \frac{1}{2\{hz/q\}}\right).$$

(由于 $\log M \gg \log P$). 由引理 3.5 及 $MP_2 \ll l'^k Q^k P_2^k = P^k \ll P_1^k L^{k(\sigma_3+\sigma_4)}$, 可得

$$\sum \ll ML^{-\sigma_2}P_2 + L^{\sigma_2}\left(\frac{M}{q}+1\right)(P_2 + q\log q)$$
$$\ll P_1^k(L^{k(\sigma_3+\sigma_4)-\sigma_2} + L^{\sigma_2+k(\sigma_3+\sigma_4)-\sigma+1}).$$

取

$$\sigma_2 = 2^{k-1}(\sigma_0+\sigma_3) + k\sigma_4 + 2^{3(k-2)} - 1,$$

则由 $\sigma \geqslant 2^k(\sigma_0+\sigma_3) + 2k\sigma_4 + 2^{3(k-2)}$ 可知

$$\sum \ll P_1^k L^{-2^{k-1}\sigma_0 - (2^{k-1}-k)\sigma_3}.$$

代入 (1) 式, 得

$$|S|^{2^{k-1}} \ll P_2^{2^{k-1}-k} P_1^k L^{-2^{k-1}\sigma_0 - (2^{k-1}-k)\sigma_3} \ll p_1^{2^{k-1}} L^{-2^{k-1}\sigma_0},$$

即

$$S \ll P_1 L^{-\sigma_0}.$$

引理 6.3　命 l 是一正整数 ($\leqslant L^{\sigma_3}$), 并命

$$\Omega = \sum_d \sum_m e(f(ldm)), \quad f(x) = \frac{h}{q}x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k,$$

此处 $(h,q)=1$, 诸 α 都是实数, $L^\sigma < q \leqslant P^k L^{-\sigma}$.$\Omega$ 中之 d 经过一适合次之条件的正整数组

$$D < d \leqslant D', \quad 1 < D < \frac{p}{l} = P_1, \quad D' \leqslant 2D.$$

又对一固定的 d, m 经过一适合次之不等式的正整数组

$$P'/d < m \leqslant P_1/d,$$

此处 P' 是一正数. 如是则当 $L^{\sigma_6} < D < PL^{-\sigma_6}$ 时, 并在条件

$$\sigma_5 \geqslant 2^{2k}\sigma_0, \quad \sigma_6 \geqslant (2k+1)\sigma_3 + 2^{2k+1}\sigma_0 + 2^{3(2k-1)}$$

及

$$\sigma \geqslant 2k\sigma_3 + 2^{2k+1}\sigma_0 + 2^{3(2k-1)}$$

之下, 我们有

$$\Omega \ll P_1 L^{-\sigma_0}.$$

证　1) 为简单起见, 命 $P_0 = [P_1/D]$. 用 Cauchy 不等式, 可知

$$\begin{aligned}|\Omega|^2 \leqslant & D\sum_d \Big|\sum_m e(f(ldm))\Big|^2 \\ \leqslant & D\sum_x \sum_m \sum_{m_1} e\left(\frac{h}{q}l^k x^k (m^k - m_1^k) + \cdots\right),\end{aligned} \tag{1}$$

此处 x 经过所有适合 $D < x \leqslant D'$ 的整数, 对一个固定的 x, m 及 m_1 经过某一适合不等式

$$\frac{P'}{x} < m \leqslant \frac{P_1}{x}, \quad \frac{P'}{x} < m_1 \leqslant \frac{P_1}{x}$$

的整数组.

变换 (1) 中和号的次序, 则得

$$|\Omega|^2 \leqslant D\sum_{m_1}\sum_m\sum_x e\left(\frac{h}{q}l^k x^k (m^k - m_1^k) + \cdots\right), \tag{2}$$

此处 m 及 m_1 经过某一适合于

$$0 < m \leqslant P_0, \quad 0 < m_1 \leqslant P_0$$

的整数列, 而对已固定的 m 及 m_1, x 经过所有适合于

$$\max\left(D, \frac{P'}{m}, \frac{P'}{m_1}\right) < x \leqslant \min\left(D', \frac{P_1}{m}, \frac{P_1}{m_1}\right)$$

的整数.

2) 写

$$\Big|\sum_m\sum_x e\left(\frac{h}{q}l^k x^k (m^k - m_1^k) + \cdots\right)\Big| \leqslant \sum_{y=1}^{P_0} S_y, \tag{3}$$

此处

$$S_y = \Big|\sum_x e\left(\frac{h}{q}l^k x^k (y^k - m_1^k) + \cdots\right)\Big|,$$

其中 x 经过在下列隔间中所有的整数:

$$\max\left(D'', \frac{p'}{y}\right) < x \leqslant \min\left(D''', \frac{P_1}{y}\right),$$

而

$$D''=\max\left(D,\frac{P'}{m_1}\right),\quad D'''=\min\left(D',\frac{P_1}{m_1}\right).$$

应用引理 3.3 及 3.4 可得

$$\begin{aligned}|S_y|^{2^k}=&\left|\sum_x e\left(\frac{h}{q}l^kx^k(y^k-m_1^k)+\cdots\right)\right|^{2^k}\\ \ll&D^{2^k-k-1}\sum_{\xi_1}^{D}\cdots\sum_{\xi_k}^{D}\sum_x^{D} e\left(\frac{h}{q}l^k(y^k-m_1^k)k!\xi_1\cdots\xi_k\right).\end{aligned}$$

对 y 求和, 并变换和号可得

$$\sum_{y=1}^{P_0}|S_y|^{2^k}\ll D^{2^k-k}\sum_{\xi_1}^{D}\cdots\sum_{\xi_k}^{D}\left|\sum_{y=1}^{P_0}e\left(\frac{h}{q}l^k(y^k-m_1^k)k!\xi_1\cdots\xi_k\right)\right|. \tag{4}$$

3) 若 $k=1$, 则

$$\begin{aligned}\sum_{y=1}^{P_0}|S_y|^2\ll&D\sum_{\xi_1}^{D}\left|\sum_{y=1}^{P_0}e\left(\frac{h}{q}ly\xi_1\right)\right|\\ \ll&D\sum_{\xi_1}^{D}\min\left(P_0,\frac{1}{\{hl\xi_1/q\}}\right)\ll D\sum_{\xi}^{Dl}\min\left(P_0,\frac{1}{\{h\xi/q\}}\right)\\ \ll&D\left(\frac{Dl}{q}+1\right)(P_0+q\log q).\end{aligned}$$

由 (2) 式 (3) 式及 Cauchy 不等式

$$\begin{aligned}|\Omega|^2\leqslant&DP_0\max_{m_1}\sum_{y=1}^{P_0}|S_y|\ll DP_0\max_{m_1}\sqrt{P_0\sum_{y=1}^{P_0}|S_y|^2}\\ \leqslant&D^2P_0^2\left(\left(\frac{l}{q}+\frac{1}{D}\right)\left(1+\frac{q\log q}{P_0}\right)\right)^{\frac12},\end{aligned}$$

即得

$$\begin{aligned}\Omega\ll&DP_0\left(\frac{l}{q}+\frac{1}{D}+\frac{l\log q}{P_0}+\frac{q\log q}{DP_0}\right)^{\frac14}\\ \ll&P_1(L^{\sigma_3-\sigma}+L^{-\sigma_5}+L^{2\sigma_3-\sigma_6+1}+L^{\sigma_3-\sigma+1})^{\frac14}\ll P_1L^{-\sigma_0}.\end{aligned}$$

此处用了

$$\sigma\geqslant\sigma_3+1+4\sigma_0,\quad\sigma_5\geqslant4\sigma_0,\quad\sigma_6\geqslant2\sigma_3+1+4\sigma_0.$$

4) 假定 $k>1$. 用 Hölder 不等式, 得

$$\left(\sum_{\xi_1}^{D}\cdots\sum_{\xi_k}^{D}\left|\sum_{y=1}^{P_0}e\left(\frac{h}{q}l^ky^kk!\xi_1\cdots\xi_k\right)\right|\right)^{2^{k-1}}$$
$$\ll D^{k(2^{k-1}-1)}\sum_{\xi_1}^{D}\cdots\sum_{\xi_k}^{D}\left|\sum_{y=1}^{P_0}e\left(\frac{h}{q}l^ky^kk!\xi_1\cdots\xi_k\right)\right|^{2^{k-1}}. \tag{5}$$

由引理 3.3, 3.4 及 1.8, 可知

$$\left|\sum_{y=1}^{P_0}e\left(\frac{h}{q}l^ky^kk!\xi_1\cdots\xi_k\right)\right|^{2^{k-1}}$$
$$\ll P_0^{2^{k-1}-k}\sum_{\eta_1}^{P_0}\cdots\sum_{\eta_{k-1}}^{P_0}\min\left(P_0,\frac{1}{2\left\{\dfrac{h}{q}l^kk!^2\xi_1\cdots\xi_k\eta_1\cdots\eta_{k-1}\right\}}\right), \tag{6}$$

因此, 由 (5) 及 (6) 得

$$\left(\sum_{\xi_1}\cdots\sum_{\xi_k}\left|\sum_{y=1}^{P_0}e\left(\frac{h}{q}l^ky^kk!\xi_1\cdots\xi_k\right)\right|\right)^{2^{k-1}}\ll D^{k(2^{k-1}-1)}P_0^{2^{k-1}-k}$$
$$\times\sum_{\xi_1}^{D}\cdots\sum_{\xi_k}^{D}\sum_{\eta_1}^{P_0}\cdots\sum_{\eta_{k-1}}^{P_0}\min\left(P_0,\frac{1}{2\left\{\dfrac{h}{q}l^k(k!)^2\xi_1\cdots\xi_k\eta_1\cdots\eta_{k-1}\right\}}\right). \tag{7}$$

5) 此和中适合

$$\xi_1\cdots\xi_k\eta_1\cdots\eta_{k-1}=0$$

的诸项之和是

$$\ll D^{k2^{k-1}}p_0^{2^{k-1}}\left(\frac{1}{D}+\frac{1}{P_0}\right)\ll D^{k2^{k-1}}P_0^{2^{k-1}}(L^{-\sigma_5}+L^{\sigma_3-\sigma_6}). \tag{8}$$

又适合

$$z=l^kk!^2\xi_1\cdots\xi_k\eta_1\cdots\eta_{k-1}$$

的项数 $\leqslant(d(z))^{2k-1}$, 且 $|z|\ll l^kk!^2D^kP_0^{k-1}$. 定义 $l^kk!^2D^kP_0^{k-1}=M$, 依照 (7), (8) 及引理 6.1, 如果 $\sigma_2>2^{3(2k-1)}-1$, 则得

$$\left(\sum_{\xi_1}\cdots\sum_{\xi_k}\left|\sum_{y=1}^{P_0}e\left(\frac{h}{q}l^ky^kk!\xi_1\cdots\xi_k\right)\right|\right)^{2^{k-1}}$$

$$\ll D^{k2^{k-1}} P_0^{2^{k-1}} (L^{-\sigma_5} + L^{\sigma_3-\sigma_6}) + D^{k2^{k-1}-k} P_0^{2^{-k}-k}$$
$$\left(ML^{-\sigma_2} P_0 + L^{\sigma_2} \sum_{0<z\ll M} \min \left(P_0, \frac{1}{2\{hz/q\}} \right) \right). \tag{9}$$

由引理 3.5 及 $M \ll L^{k\sigma_3} D^k P_0^{k-1}$, 可得

$$\sum_{0<z\ll M} \min \left(P_0, \frac{1}{2\{hz/q\}} \right) \ll \left(\frac{M}{q} + 1 \right) (P_0 + q \log q)$$
$$\ll D^k P_0^k (L^{1+k\sigma_3-\sigma} + L^{(k+1)\sigma_3-\sigma_6+1}).$$

代入 (9) 式, 立得

$$\left(\sum_{\xi_1} \cdots \sum_{\xi_k} \left| \sum_{y=1}^{P_0} e\left(\frac{h}{q} l^k k! \xi_1 \cdots \xi_k (y^k - m_1^k) \right) \right| \right)^{2^{k-1}}$$
$$\ll D^{k2^{k-1}} P_0^{2^{k-1}} (L^{-\sigma_5} + L^{\sigma_3-\sigma_6} + L^{\sigma_2+1+k\sigma_3-\sigma} + L^{\sigma_2+(k+1)\sigma_3-\sigma_6+1}).$$

6) 取

$$\sigma_2 = k\sigma_3 + 2^{2k}\sigma_0 + 2^{3(2k-1)} - 1.$$

由于

$$\sigma_5 \geqslant 2^{2k}\sigma_0, \sigma_6 \geqslant (2k+1)\sigma_3 + 2^{2^{k+1}}\sigma_0 + 2^{3(2k-1)}$$

及

$$\sigma > 2k\sigma_3 + 2^{2^{k+1}}\sigma_0 + 2^{3(2^k-1)},$$

可得

$$\sum_{\xi_1} \cdots \sum_{\xi_k} \left| \sum_{y=1}^{P_0} e\left(\frac{h}{q} l^k k! \xi_1 \cdots \xi_k (y^k - m_1^k) \right) \right| \ll D^k P_0 L^{-2^{k+1}\sigma_0}$$

由 (4) 得

$$\sum_{y=1}^{P_0} |S_y|^{2^k} \ll D^{2^k} P_0 L^{-2^{k+1}\sigma_0}.$$

用 Hölder 不等式, 得出

$$\sum_{y=1}^{P_0} |S_y| \leqslant P_0^{1-2^{-k}} \left(\sum_{y=1}^{P_0} |S_y|^{2^k} \right)^{2^{-k}} \ll DP_0 L^{-2\sigma_0}$$

再由 (2) 式得出

$$|\Omega|^2 \leqslant DP_0 DP_0 L^{-2\sigma_0}$$

及

$$\Omega \ll DP_0 L^{-\sigma_0} \ll P_1 L^{-\sigma_0}.$$

§6.3　定理的证明

1) 以 H 代表所有不大于 $\sqrt{P}$ 的素数的乘积. 以 (d) 表 H 的除数所成的数集. 运用一习知的论证法, 可知

$$S=\sum_{(d)\leqslant P}\mu(d)S_d+O(\sqrt{P}),$$

此处 $\mu(d)$ 是 Möbius 函数而

$$S_d=\sum_{\substack{dm\leqslant P\\ dm\equiv t(\bmod Q)}}e(f(dm)).$$

2) 今先估计

$$S_0=\sum_{(d)\leqslant L^{\lambda_1}}\mu(d)S_d,\quad \lambda_1=2^{2k}(\sigma_0+\sigma_1+1)$$

的值. 在引理 6.2 中取 $l=d,\sigma_3=\lambda_1,\sigma_4=\sigma_1$ 及 σ_0+1 代替 σ_0, 则得

$$|S_d|\ll\frac{P}{Qd}L^{-\sigma_0-1}$$

(此处用了 $\sigma\geqslant 2k\sigma_1+2^k(\sigma_0+1+\lambda_1)+2^{3(k-2)}$). 故

$$S_0\leqslant\sum_{d\leqslant L^{\lambda_1}}\frac{P}{Qd}L^{-\sigma_0-1}\ll PQ^{-1}L^{-\sigma_0}.$$

3) 以 (d_0) 表 (d) 中有偶数个素因子的数所成的数集, 而 (d_1) 表其余部分. 命

$$S'=\sum_{L^{\lambda_1}<(d)\leqslant P}\mu(d)S_d=T_0-T_1,$$

此处

$$T_0=\sum_{L^{\lambda_1}<(d_0)\leqslant P}S_{d_0},\quad T_1=\sum_{L^{\lambda_1}<(d_1)\leqslant P}S_{d_1}.$$

今后研究 T_0, 因为 T_1 可以由同法得出相似的结果.

4) 讨论 T_0 的一部分

$$T_0'=\sum_{L^{\lambda_1}<(d_0)\leqslant PL^{-\lambda_2}}S_{d_0},\quad \lambda_2=2^{2^{k+1}}(\sigma_0+\sigma_1+1)+2^{3(2k-1)}.$$

将此和分为 $O(L)$ 份, 每一份和的形式如

$$D < d \leqslant D', \quad D' \leqslant 2D.$$

以 Ω 代表其中之一, 如此则

$$\Omega = \sum_d \sum_m e(f(dm)),$$

此处 d 经过某一适合于

$$D < d \leqslant D', \quad D' \leqslant 2D, \quad L^{\lambda_1} < D \leqslant PL^{-\lambda_2}$$

的数列. 对已定的 d, m 经过适合于

$$0 < m \leqslant \frac{P}{d}, \quad md \equiv t \pmod{Q}$$

的数列.

在引理 6.3 中取 $l = 1, \sigma_3 = 0, \sigma_5 = \lambda_1, \sigma_6 = \lambda_2$ 及以 $\sigma_0 + \sigma_1 + 1$ 代 σ_0, 则由 $\sigma \geqslant 2^{2k+1}(\sigma_0 + \sigma_1 + 1) + 2^{3(2k-1)}$, 可得

$$\Omega \ll PL^{-\sigma_0 - 1 - \sigma_1}.$$

由是即得

$$T_0' \ll L|\Omega| \ll \frac{P}{Q} L^{-\sigma_0}.$$

5) 所留待讨论之部分可以写成

$$T_0'' = \sum_d \sum_m e(f(dm)),$$

此处 d 经过 (d_0) 中适合

$$PL^{-\lambda_2} < d \leqslant P$$

的整数, 且对一固定的 d, m 经过适合

$$0 < m \leqslant P/d, \quad md \equiv t \pmod{Q}$$

的整数. 换和号, 则得

$$T_0'' = \sum_m T(m), \quad T(m) = \sum_d e(f(dm)),$$

此处 m 经过整数

$$m = 1, 2, \cdots, [L^{\lambda_2}],$$

而对一固定的 m, d 则经过一适合于

$$PL^{-\lambda_2} < d \leqslant \frac{P}{m}$$

的整数组.

6) 以 (d_0') 表 (d_0) 之分集, 其中整数有素因子 $\geqslant L^{\lambda_3}$ 者 $(\lambda_3 = \sigma_0 + \lambda_2 + \sigma_1)$; 而 (d_0'') 表其余部分. 则

$$T(m) = T'(m) + T''(m), \quad T'(m) = \sum_{(d_0')}, \quad T''(m) = \sum_{(d_0'')}.$$

(d_0'') 中适合于 $PL^{-\lambda_2} < d \leqslant \dfrac{P}{m}$ 的元素的个数小于适合以下条件的整数 l 的个数 F : $(i) l$ 无大于一的平方因子, (ii)l 适合不等式

$$P^{\frac{1}{2}} < l < P,$$

(iii)l 的素因子不大于 L^{λ_3}. 假定 l 有 s 个素因子, 则

$$L^{s\lambda_3} \geqslant l > P^{\frac{1}{2}},$$

由此得出 $s \geqslant \dfrac{1}{2}L/(\lambda_3 \log L)$. 又

$$d(l) = 2^s > 2^{\frac{1}{2}L/(\lambda_3 \log L)} \gg L^{\lambda_3+1}.$$

由引理 2.5.

$$FL^{\lambda_3+1} \leqslant \sum_{l=1}^{P} d(l) \ll PL,$$

即

$$F \ll PL^{-\lambda_3}.$$

故得

$$T(m) = T'(m) + O(PL^{-\lambda_3}) = T'(m) + O\left(\frac{P}{Q}L^{-\sigma_0-\lambda_2}\right).$$

(此处用了 $\lambda_3 = \sigma_0 + \lambda_2 + \sigma_1$).

7) 以 $T_s(m)$ 表一和, 其 d 经过 (d_0') 的一分集, 其中元素恰有 s 个素因子 $\geqslant L^{\lambda_3}$. 由于

$$L^{\lambda_3 s} \leqslant P, \quad s \leqslant \frac{L}{\lambda_3 \log L} < L,$$

故得

$$T'(m) = \sum_{s<L} T_s(m),$$

而

$$T_s(m)=\sum_d e(f(md))$$

乃一和, 其中所经过的 d 适合于不等式

$$PL^{-\lambda_2}<d\leqslant P_1=\frac{P}{m},\quad md\equiv t(\bmod Q),$$

且 d 乃 (d_0') 之一员, 并恰有 s 个素因子 $\geqslant L^{\lambda_3}$.

8) 因为要估计, 我们引进一和

$$T_{s0}(m)=\sum_u\sum_v e(f(muv)),$$

此处 u 经过所有 $\geqslant L^{\lambda_3}$ 的素数且在 (d) 中, 对已与的 u,v 经过所有适合不等式

$$\frac{PL^{-\lambda_2}}{u}<v\leqslant\frac{P_1}{u},\quad muv\equiv t\quad(\bmod Q)$$

的整数, 且 v 在 (d_1) 中, 并恰有 $s-1$ 个素因子 $\geqslant L^{\lambda_3}$.

在 $T_s(m)$ 中每一项 $e(f(m\ d))$ 在 $T_{s0}(m)$ 中出现 s 次. 舍此而外, $T_{s0}(m)$ 中不在 $T_s(m)$ 中出现的项的形式如

$$e(f(mp^2v_1)),\quad\frac{PL^{-\lambda_2}}{p^2}<v_1\leqslant\frac{P_1}{p^2},$$

此处 $p\leqslant L^{\lambda_3}$, 而 v_1 经过 (d_0) 中之元素, 且 v_1 恰有 $s-2$ 个素因子 $\geqslant L^{\lambda_3}$. (当 $s=1$, 则此类项不存在). 如此的项在 $T_{s0}(m)$ 中出现的次数仅一次且唯一次 (因为 v_1 无平方因子). 对一已与之 p, 共有 $\ll P_1/p^2$ 项, 所以

$$T_{s0}(m)=sT_s(m)+O\left(\sum_{p\geqslant L^{\lambda_3}}\frac{P_1}{p^2}\right)=sT_s(m)+O\left(\frac{P}{m}L^{-\lambda_3}\right).$$

故

$$T_s(m)=\frac{1}{s}T_{s0}(m)+O\left(\frac{P}{ms}L^{-\lambda_3}\right).$$

9) 把引理 6.3 用到 $T_{s0}(m)$ 上. 和

$$T_{s0}(m)=\sum_u\sum_v e(f(m\ u\ v))$$

中 u 乃经过 $L^{\lambda_3}\leqslant u\leqslant\sqrt{P}$ 间所有的素数. 对一固定的 u, 变数 v 经过 (d_1) 中所有适合以下诸条件的元素:

(i) v 恰有 $s-1$ 个素因子 $\geqslant L^{\lambda_3}$,

(ii) $PL^{-\lambda_2}/u < v \geqslant P_1/u$,

(iii) $muv \equiv t(\bmod Q)$.

把 $L^{\lambda_3} \leqslant u \leqslant \sqrt{P}$ 分成 $O(L)$ 份, 使其每一份皆可以应用引理 6.3. 今于引理 6.3 中取 $l=m, \sigma_3=\lambda_2, \sigma_5=\lambda_3$, 并取 σ_6 为一任意大之整数, 且用 $\sigma_1+\sigma_0+2$ 代替 σ_0. 如是则由

$$\lambda_3 \geqslant 2^{2k}(\sigma_1+\sigma_0+2), \quad \sigma \geqslant 2k\lambda_2 + 2^{2k+1}(\sigma_1+\sigma_0+2)+2^{3(2k-1)}$$

可得

$$T_{s^0}(m) \ll \frac{P}{m}L^{-\sigma_0-\sigma_1-2}L = \frac{P}{m}L^{-\sigma_0-\sigma_1-1}.$$

因此得到

$$T_s(m) \ll \frac{P}{sm}L^{-\sigma_0-\sigma_1-1} + \frac{P}{sm}L^{-\lambda_3} \ll \frac{P}{sm}L^{-\sigma_0-\sigma_1-1}.$$

此处用上了 $\lambda_3 \geqslant \sigma_0+\sigma_1+1$.

最后,

$$\begin{aligned}
T_0 =& T_0' + T_0'' = T_0' + \sum_m T(m) \ll T_0' + \sum_m T'(m) + \sum_m \frac{P}{Q}L^{-\sigma_0-\lambda_2} \\
\ll& \frac{P}{Q}L^{-\sigma_0} + \sum_m \sum_{s<L} T_s(m) \ll \frac{P}{Q}L^{-\sigma_0} + \sum_m \sum_{s<L} \frac{P}{Qsm}L^{-\sigma_0-1} \\
\ll& \frac{P}{Q}L^{-\sigma_0}.
\end{aligned}$$

由此得到

$$S \ll \frac{P}{Q}L^{-\sigma_0}.$$

第 7 章　华林–哥德巴赫问题的解数的渐近式

§7.1

命 $f(x)$ 表一 k 次的整值多项式, 其最高项系数 A 是正数. 并假定无整数 $q(>1)$ 存在使对所有的 x 恒有 $f(x)\equiv f(0)(\bmod q)$. 以 $I_s(N)$ 表方程

$$f(p_1)+\cdots+f(p_s)=N$$

的解答数, 其中未知数 $p_1,\cdots,p_s$ 是素数. (为简单计, 这一问题称为华林–哥德巴赫问题.) 本章之目的在证明下之定理:

定理 11　若

$$s\geqslant\begin{cases}2^k+1, & \text{当}1\leqslant k\leqslant 10,\\ 2k^2(2\log k+\log\log k+2.5), & \text{当}k>10,\end{cases}$$

则

$$\left|I_s(N)-A^{-sa}\mathfrak{S}(N)\frac{\Gamma^s(a)}{\Gamma(sa)}\frac{N^{sa-1}}{(\log N)^s}\right|\leqslant\frac{c(k,s,f\text{的系数})N^{sa-1}}{(\log N)^{s+1}}\log\log N,$$

此处

$$\mathfrak{S}(N)=\sum_{q=1}^{\infty}B_s(N,q),$$

$$B_s(N,q)=\sum_{\substack{h=1\\(h,q)=1}}\left(\frac{W_h,q}{\varphi(\bar{q})}\right)^s e_q(-hN),$$

$$W_{h,q}=\sum_{\substack{l=1\\(l,q)=1}}e_q(hf(l)),$$

而 $\bar{q}=q\prod\limits_{p|q,p^t||d}p^t, d$ 为 $f(x)$ 的系数之最小公分母.

在证明定理 11 时我们需要一重要引理: 命 $r_{2t}(P)$ 表方程

$$f(x_1)+\cdots+f(x_t)=f(y_1)+\cdots+f(y_t),\quad 0\leqslant x,y\leqslant P,$$

的整数解答 $x_1,\cdots,x_t,y_1,\cdots,y_t$ 的组数, 则当 $k\geqslant 11$,

$$2t>k^2(2\log k+\log\log k+2.5)-2$$

时,

$$r_{2t} = \int_0^1 |T(\alpha)|^{2t} d\alpha \ll P^{2t-k}, \quad T(\alpha) = \sum_{x=1}^{P} e(f(x)\alpha).$$

§7.2 若 干 引 理

引理 7.1 命 $\tau \geqslant 1$. 对任一实数 α 有二整数 h 及 q 存在, 使

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{1}{q\tau}, \quad 0 < q < \tau, \quad (h, q) = 1.$$

证 并不失去普遍性, 我们可以假定 $\alpha > 0$. 把 α 展开成连分数, 且命

$$\frac{P_1}{Q_1} = \frac{[\alpha]}{1}, \quad \frac{P_2}{Q_2}, \quad \frac{P_3}{Q_3}, \quad \cdots$$

表它的渐近分数, 数列 Q_ν 或有止境, 或趋向无穷. 若止于 $P_s/Q_s, Q_s \leqslant \tau$, 则 $\alpha = P_s/Q_s$, 此引理显然正确. 若有一 m 使

$$Q_m < \tau \leqslant Q_{m+1},$$

则

$$\left|\alpha - \frac{P_m}{Q_m}\right| \leqslant \left|\frac{P_{m+1}}{Q_{m+1}} - \frac{P_m}{Q_m}\right| = \frac{1}{Q_m Q_{m+1}} \leqslant \frac{1}{Q_m \tau},$$

即得本引理, 其中 $h = P_m, q = Q_m$.

引理 7.2 (Euler 求和式). 命

$$b_1(x) = x - [x] - \frac{1}{2}.$$

用归纳法定义次之函数:

$$b_l(x+1) = b_l(x), \tag{1}$$

$$\int_0^x b_l(y)\mathrm{d}y = b_{l+1}(x) - b_{l+1}(0). \tag{2}$$

命 $b > a$. 在隔间 $a \leqslant x \leqslant b$ 中, 设 $g(x)$ 是一具有多次导数的函数, 其次数视我们的需要而定. 则对所有的 t

$$\sum_{\substack{m \\ a \leqslant m+t < b}} g(m+t) = \int_a^b g(x)\mathrm{d}x$$

$$+ \sum_{r=0}^{l-1} (g^{(r)}(b) b_{r+1}(t-b) - g^{(r)}(a) b_{r+1}(t-a))$$

$$-\int_a^b g^{(l)}(x)b_l(t-x)\mathrm{d}x. \tag{3}$$

证　1) 简化引理：

1.1) 我们不妨假定 $t=0$. 因为我们取 $a-t=A, b-t=B, g(x+t)=G(x)$, 则有

$$\begin{aligned}\sum_{A\leqslant m<B} G(m) = &\int_A^B G(x)\mathrm{d}x \\ &+\sum_{r=0}^{l-1}(G^{(r)}(B)b_{r+1}(-B)-G^{(r)}(A)b_{r+1}(-A)) \\ &-\int_A^B G^{(l)}(x)b_l(-x)\mathrm{d}x.\end{aligned}$$

1.2) 因为上式的每边都是可加的, 所以只须证明

$$w\leqslant A<B\leqslant w+1$$

时的情况即可, 此处 w 是任一整数.

1.3) 如 1.1) 所论, 我们可以假定 $w=0$ 而不失其普遍性.

2) 当 $l=1$ 时, 引理真实. 即

$$\begin{aligned}G(0)=&\int_0^B G(x)\mathrm{d}x+G(B)b_1(-B)-G(0)b_1(0) \\ &-\int_0^B G'(x)b_1(-x)\mathrm{d}x, \quad 当 A=0\end{aligned} \tag{4}$$

及

$$\begin{aligned}0=&\int_A^B G(x)\mathrm{d}x+G(B)b_1(-B)-G(A)b_1(-A) \\ &-\int_A^B G'(x)b_1(-x)\mathrm{d}x, \quad 当 0<A<B\leqslant 1.\end{aligned} \tag{5}$$

此二式的证明如下：

$$\begin{aligned}\int_A^B G'(x)b_1(-x)\mathrm{d}x &= \int_A^B G'(x)\left(-x-[-1]-\frac{1}{2}\right)\mathrm{d}x \\ &=\left[\left(-x+\frac{1}{2}\right)G(x)\right]_A^B+\int_A^B G(x)\mathrm{d}x \\ &=\int_A^B G(x)\mathrm{d}x+\left(-B+\frac{1}{2}\right)G(B)-\left(-A+\frac{1}{2}\right)G(A)\end{aligned}$$

$$= \int_A^B G(x)\mathrm{d}x + b_1(-B)G(B)$$

$$-b_1(-A)G(A) - \begin{cases} 0, & 若A \neq 0, \\ G(A), & 若A = 0, \end{cases}$$

由于 $\frac{1}{2} = -\frac{1}{2} + 1 = b_1(0) + 1.$

3) 归纳法. 运用分部积分法, 可得

$$-\int_A^B G^{(l)}(x)b_l(-x)\mathrm{d}x = G^{(l)}(B)b_{l+1}(-B) - G^{(l)}(A)b_{l+1}(-A) - \int_A^B G^{(l+1)}(x)b_{l+1}(-x)\mathrm{d}x.$$

引理已经证明.

引理 7.3　在任一有限的间隔中 $b_l(x)$ 是一囿变函数.

证　当 $l = 1$ 时, 在 (0,1) 中 $b_1(x)$ 是二单调函数之差, 因之, 它是囿变函数. 对于一般的情况, 可由 $b_l(x)$ 是 $b_{l-1}(x)$ 的积分这一性质得出.

引理 7.4　若 $x \neq [x]$, 则

$$b_1(x) = x - [x] - \frac{1}{2} = -\frac{1}{\pi}\sum_{n=1}^{\infty}\frac{\sin 2\pi nx}{n}.$$

证　只须讨论 $0 < x < 1$ 时的情况即可. 因

$$\log(1-z) = -\left(z + \frac{z^2}{2} + \cdots + \frac{z^n}{n} + \cdots\right),$$

故 $\frac{1}{\pi \mathrm{i}}\log(1-\mathrm{e}^{2\pi \mathrm{i}x})$ 的级数的实数部分等于引理中之右边, 而 $\frac{1}{\pi i}\log(1-\mathrm{e}^{2\pi ix})$ 的实数部分等于

$$-\frac{1}{\pi}\arctan\frac{\sin 2\pi x}{1-\cos 2\pi x} = x - \frac{1}{2}.$$

引理即已证明.

引理 7.5　命 $b > a$. 假定 $\varphi(x)$ 和 $f'(x)$ 是隔间 (a, b) 中连续的实函数, 在此隔间中仅有有限个*极大值和极小值. 则

1)

$$\int_a^b \varphi(x)e(x)\mathrm{d}x \ll \max_{0\leqslant\xi\leqslant 1}\max_{a\leqslant v\leqslant b-\xi}\int_v^{v+\xi}|\varphi(x)|\mathrm{d}x. \tag{6}$$

* 所谓有限个极大值和极小值, 乃指其个数不超过一个仅与 k 相关的数.

2) 假定 $f(x)$ 可求微分且适合 $|f'(x)| \leqslant \frac{1}{2}$. 则

$$\sum_{a\leqslant x\leqslant b} \mathrm{e}^{2\pi \mathrm{i} f(x)} - \int_a^b \mathrm{e}^{2\pi \mathrm{i} f}(x)\mathrm{d}x \ll 1. \tag{7}$$

证　1) 当 $b-a\leqslant 1$ 时, 本引理 1) 显然真实.

现在假定 $a<b-1$. 如能证明

$$\int_a^b \varphi(x)e(x)\mathrm{d}x \ll \max_{a\leqslant v\leqslant b-1}\int_v^{v+1}|\varphi(x)|\mathrm{d}x, \tag{8}$$

则引理已经证明. 我们也可以假定 $\varphi(x)$ 是单调的, 而不失其普遍性. 如若不然, 我们可以分此隔间成为有限段, 每一段中 $\varphi(x)$ 是单调的. 由于方法相同, 我们仅讨论 $\varphi(x)$ 是递减时的情况. 因为

$$\left|\int_a^b \varphi(x)e(x)\mathrm{d}x\right| \leqslant \int_a^{[a]+1}|\varphi(x)|\mathrm{d}x + \left|\int_{[a]+1}^{[b]}\varphi(x)e(x)\mathrm{d}x\right| + \int_{[b]}^b|\varphi(x)|\mathrm{d}x,$$

所以我们只须证明 (8) 式当 a 及 b 都是整数的情形即可.

我们现在有

$$\begin{aligned}\int_a^b \varphi(x)\sin 2\pi x\mathrm{d}x &= \int_a^{a+\frac{1}{2}}\varphi(x)\sin 2\pi x\mathrm{d}x + \int_{a+\frac{1}{2}}^{a+1}\varphi(x)\sin 2\pi x\mathrm{d}x + \cdots\\ &= \int_0^{\frac{1}{2}}\left(\varphi(x+a) - \varphi\left(x+a+\frac{1}{2}\right) + \varphi(x+a+1) - \cdots\right.\\ &\quad \left. - \varphi\left(x+b-\frac{1}{2}\right)\right)\sin 2\pi x\mathrm{d}x.\end{aligned}$$

因为 $\varphi(x)$ 是递减函数, 所以

$$0\leqslant \varphi(x+a) - \varphi\left(x+a+\frac{1}{2}\right) + \varphi(x+a+1) - \cdots - \varphi\left(x+b-\frac{1}{2}\right) \leqslant \varphi(x+a).$$

由此立得

$$\begin{aligned}0 &\leqslant \int_a^b \varphi(x)\sin 2\pi x\mathrm{d}x \leqslant \int_0^{\frac{1}{2}}\varphi(x+a)\sin 2\pi x\mathrm{d}x\\ &\leqslant \int_0^{\frac{1}{2}}|\varphi(x+a)|\mathrm{d}x \leqslant \int_a^{a+\frac{1}{2}}|\varphi(x)|\mathrm{d}x.\end{aligned}$$

用同样方法来讨论

$$\int_a^b \varphi(x)\cos 2\pi x\mathrm{d}x,$$

并将所得的结果合并, 即得出本引理 1).

2) 如 1) 的论点我们仍可以假定 $f'(x)$ 是单调的. 现估计积分

$$\int_a^b f'(x)\mathrm{e}^{2\pi\mathrm{i}(f(x)\pm mx)}\mathrm{d}x, \quad m\text{是整数}.$$

命 $f(x)\pm mx=y$, 则此积分等于

$$\int \frac{f'(x)}{f'(x)\pm m}\mathrm{e}^{2\pi\mathrm{i}y}\mathrm{d}y.$$

由 1) 可以算出

$$\left|\int_a^b f'(x)\mathrm{e}^{2\pi\mathrm{i}(f(x)\pm mx)}\mathrm{d}x\right|\leqslant\int\left|\frac{f'(x)}{m\pm f'(x)}\right|\mathrm{d}y\ll\frac{1}{m}.$$

由此立刻有

$$\int_a^b \mathrm{e}^{2\pi\mathrm{i}f(x)}f'(x)\sin 2\pi mx\mathrm{d}x=O\left(\frac{1}{m}\right).$$

由引理 7.4 可得

$$\begin{aligned}\left|\int_a^b \mathrm{e}^{2\pi\mathrm{i}f(x)}f'(x)b_1(-x)\mathrm{d}x\right|=&\frac{1}{\pi}\left|\int_a^b \mathrm{e}^{2\pi\mathrm{i}f(x)}f'(x)\sum_{m=1}^{\infty}\frac{\sin 2\pi mx}{m}\mathrm{d}x\right|\\ =&\frac{1}{\pi}\left|\sum_{m=1}^{\infty}\frac{1}{m}\int_a^b \mathrm{e}^{2\pi\mathrm{i}f(x)}f'(x)\sin 2\pi mx\mathrm{d}x\right|\\ =&O\left(\sum_{m=1}^{\infty}\frac{1}{m^2}\right)=O(1)\end{aligned}$$

(逐项求积分时, 运用了 $b_1(-x)$ 的级数是囿收敛这一点).

最后, 由 Euler 的求和公式即可得出我们的引理.

引理 7.6 　命 $\Psi_1(x)=\mathrm{e}^{\mathrm{i}x^k}$. 则

$$\Psi_1^{(r)}(x)=\mathrm{e}^{\mathrm{i}x^k}F_r(x),$$

此处 $F_r(x)$ 是一 $(k-1)r$ 次的多项式.

此引理的证明用归纳法不难得出.

引理 7.7 　命 $\Psi(x)=e(\beta A(qx)^k)$. 若 $q\leqslant c_1(k)P^{1-\varepsilon}$, $|\beta|\leqslant c_2(k)q^{-1}P^{-k+1-\varepsilon}$ 及 $0\leqslant x\leqslant P/q$, 则

$$|\Psi^{(r)}(x)|\leqslant c_3(A,\varepsilon,r,k)P^{-r\varepsilon}.$$

证 　由

$$|\beta|^a q\leqslant(c_2(k))^a q^{1-a}P^{-1+a-\varepsilon a}$$

$$\leqslant (c_2(k))^a (c_1(k))^{1-a} P^{(1-\varepsilon)(1-a)-1+a-\varepsilon a}$$

及

$$(|\beta|^a q)^k x^{k-1} \leqslant |\beta| q^k \left(\frac{P}{q}\right)^{k-1} \leqslant c_2(k) P^{-\varepsilon},$$

由引理 7.6, 可知

$$\begin{aligned}|\Psi^{(r)}(x)| &= |\Psi(x) F_r((2\pi\beta A)^a qx)((2\pi i\beta A)^a q)^r| \\ &\leqslant c_4(A,\varepsilon,r,k)(1+(|\beta|^a qx)^{(k-1)r})(|\beta|^a q)^r \\ &\leqslant c_3(A,\varepsilon,r,k) P^{-r\varepsilon}.\end{aligned}$$

引理 7.8　命 $f(x) = A_k x^k + \cdots + A_1 x + A_0$,

$$\Phi(x) = e(\beta f(qx)).$$

则在引理 7.7 的条件下

$$|\Phi^{(r)}(x)| \leqslant c_5(A_k, \cdots, A_0, \varepsilon, r, k) P^{-r\varepsilon}.$$

证　当 $k=1$ 时引理显然成立. 命

$$\Phi(x) = \Psi(x)\Phi_1(x), \quad \Phi_1(x) = e(\beta f(qx) - \beta A_k (qx)^k).$$

假定此引理对 $k-1$ 时真实. 即当 $|\beta| \ll q^{-1} P^{-k+2-\varepsilon}$ 时

$$|\Phi_1^{(r)}(x)| \leqslant c_6(A_{k-1}, \cdots, A_0, \varepsilon, r, k) P^{-r\varepsilon}.$$

由于 $q^{-1}P^{-k+2-\varepsilon} > q^{-1}P^{-k+1-\varepsilon}$, 则当 $|\beta| \leqslant c_2(k) q^{-1} P^{-k+1-\varepsilon}$ 时

$$|\Phi_1^{(r)}(x)| \leqslant c_6 P^{-r\varepsilon}.$$

故由

$$\Phi^{(r)}(x) = \Psi^{(r)}(x)\Phi_1(x) + \binom{r}{1} \Psi^{(r-1)}(x)\Phi_1'(x) + \cdots + \Psi(x)\Phi_1^{(r)}(x)$$

可得出

$$|\Phi^{(r)}(x)| \leqslant c_5 P^{-r\varepsilon}.$$

§7.3　Farey 分割

命 $k>2$. 对隔间 $-\frac{1}{\tau}\leqslant\alpha\leqslant 1-\frac{1}{\tau}$ 中任一数 α, 由引理 7.1 已知有一对整数 h 及 q 使

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{1}{q\tau},\quad 0<q<\tau,\quad (h,q)=1,$$

此处 $\tau=P^{k-1+\varepsilon}$.

在隔间 $\left(-\frac{1}{\tau},1-\frac{1}{\tau}\right)$ 中任一有理点 $\frac{h}{q}$ 附近做一分隔间

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{1}{q\tau}.$$

对 $q\leqslant P^{1-\varepsilon}$ 的分隔间用 $\mathfrak{M}(h,q)$ 表之. 隔间 $\left(-\frac{1}{\tau},1-\frac{1}{\tau}\right)$ 中之点不在任一分隔间 $\mathfrak{M}(h,q)$ 之中者以 E 表之.

今证任二 $\mathfrak{M}(h,q)$ 都无公共之点. 若不然, 设

$$\alpha=\frac{h}{q}+\beta,\quad \alpha=\frac{h_1}{q_1}+\beta_1,\quad |\beta|\leqslant\frac{1}{q\tau},\quad |\beta_1|\leqslant\frac{1}{q_1\tau},$$

则

$$\left|\frac{h_1}{q_1}-\frac{h}{q}\right|=|\beta_1-\beta|,\quad \text{即}\,\frac{1}{qq_1}\leqslant\frac{1}{q\tau}+\frac{1}{q_1\tau},\quad 1\leqslant\frac{q_1+q}{\tau}.$$

由于 $q+q_1\leqslant 2P^{1-\varepsilon}$, 故此为不可能.

因此, 命

$$T(\alpha)=\sum_{x=1}^{P}e(f(x)\alpha),$$

则当 P 充分大时有

$$\begin{aligned}r_{2t}(P)=\int_0^1|T(\alpha)|^{2t}\mathrm{d}\alpha&=\int_{-\frac{1}{\tau}}^{1-\frac{1}{\tau}}|T(\alpha)|^{2t}\mathrm{d}\alpha\\&=\int_E|T(\alpha)|^{2t}\mathrm{d}\alpha+\sum_{q\leqslant P^{1-\varepsilon}}\sum_{\substack{h=1\\(h,q)=1}}^{q}\int_{\mathfrak{M}(h,q)}|T(\alpha)|^{2t}\mathrm{d}\alpha.\end{aligned}$$

§7.4　估计展在 E 上的积分的绝对值

引理 7.9　当 $k\geqslant 12$ 及 $t>k^2(2\log k+\log\log k+2.5)-2$ 时,

$$\int_E|T(\alpha)|^{2t}\mathrm{d}\alpha\ll P^{2t-k}.$$

证　由定理 6 及 9, 命 $t = t_1 + t_2$, 可得

$$\int_E |T(\alpha)|^{2t}\mathrm{d}\alpha \ll P^{2(1-1/\sigma_k)t_2+2t_1-k+\delta+\varepsilon}$$
$$\ll P^{2t-k+\delta-2t_2/\sigma_k+\varepsilon}.$$

令取 $t_2 = 2k^2$, 及

$$l = \left[\frac{\log\left(\frac{1}{2}k(k+1)\log k^2\right)}{-\log(1-a)} + 1\right].$$

如此则

$$\delta = \frac{1}{2}k(k+1)(1-a)^l < \frac{1}{2\log k},$$

而

$$\frac{2t_2}{\sigma_k} = \frac{4k^2}{2k^2(2\log k + \log\log k + 3)} > \frac{1}{2\log k}.$$

因此, 如能证明

$$\frac{1}{4}(k^2+k+2) + lk + 2k^2 \leqslant k^2(2\log k + \log\log k + 2.5) - 2,$$

则立刻得出本引理.

由

$$l \leqslant \frac{\log\left(\frac{1}{2}k(k+1)\log k^2\right)}{-\log(1-a)} + 1 \leqslant \left(1-\frac{a}{2}\right)k\log(k^2\log k) + 2$$
$$\leqslant k\log(k^2\log k) - \log k - \frac{1}{2}\log\log k + 2,$$

可知

$$\frac{1}{4}(k^2+k+2) + lk + 2k^2 \leqslant k^2(2\log k + \log\log k + 2.5) - 2.$$

因此证明了本引理.

§7.5　关于 $\mathfrak{M}(h,q)$ 的引理

命

$$T^*(\alpha,h,q) = \bar{q}^{-1}S_{h,q}\int_0^P e(f(y)\beta)\mathrm{d}y,$$

此处

$$S_{h,q}=\sum_{v=1}^{\bar{q}}e_q(hf(v)),\quad \bar{q}=q\prod_{p|q,p^t\|d}p^t.$$

此处 d 乃 $f(x)$ 的系数的最小公分母.

引理 7.10

$$T^*(\alpha,h,q)\ll q^{-\alpha+\varepsilon}\min(P.|\beta|^{-a}).$$

证 由定理 1(推理 1.2) 已知

$$S_{h,q}\ll q^{1-a+\varepsilon}.$$

又因为 $\int_0^P e(\beta f(y))\mathrm{d}y=O(P)$, 所以我们所待证明的是下面的结论：当 $|\beta|^{-a}\leqslant P$ 时,

$$\int_0^P e(\beta f(y))\mathrm{d}y\ll|\beta|^{-a}.$$

存在一常数 c 使

$$f(y+c)=g(y)$$

是一正系数的多项式. 如此则

$$\int_c^P e(\beta f(y))\mathrm{d}y=\int_{|\beta|^{-a}}^{P-c}e(\beta g(y))\mathrm{d}y+O(|\beta|^{-a}).$$

命 $w=|\beta|g(y)$. 则 y 可以看成是 w 的递增函数. 命 $w_0=|\beta|g(|\beta|^{-a})$. 则由第二中值定理可知

$$\int_{w_0}\frac{\mathrm{e}^{\pm2\pi\mathrm{i}w}}{|\beta|g'(y)}\mathrm{d}w\ll\left(\frac{1}{|\beta|g'(y)}\right)_{w=w_0}\ll\frac{1}{|\beta|^a}.$$

引理 7.11 命 $\alpha=\dfrac{h}{q}+\beta$. 当 $q\leqslant P^{1-\varepsilon}$ 及 $|\beta|\leqslant q^{-1}P^{-k+1-\varepsilon}$ 时,

$$T(\alpha)-T^*(\alpha,h,q)\ll q^{1-a+\varepsilon}.$$

证 我们有

$$\begin{aligned}T(\alpha)&=\sum_{x=1}^{P}e(f(x)\alpha)\\&=\sum_{v=1}^{\bar{q}}\sum_{\substack{0<r\leqslant P\\ r\equiv v(\mathrm{mod}\,\bar{q})}}e\left(\frac{h}{q}f(r)\right)e(\beta f(r))\end{aligned}$$

$$=\sum_{v=1}^{\bar{q}} e\left(\frac{h}{q}f(v)\right)\Lambda_v,$$

此处

$$\Lambda_v=\sum_{\substack{j\\0<\bar{q}j+v\leqslant P}} e(\beta f(\bar{q}j+v))=\sum_{\substack{j\\0<j+\frac{v}{\bar{q}}\leqslant\frac{P}{\bar{q}}}}\Phi\left(j+\frac{v}{\bar{q}}\right),$$

及

$$\Phi(x)=e(\beta f(\bar{q}x)).$$

运用引理 7.2, 得

$$\Lambda_v=\int_0^{P/\bar{q}}\Phi(x)\mathrm{d}x+\sum_{r=1}^{l-1}\left(\Phi^{(r)}\left(\frac{P}{\bar{q}}\right)b_{r+1}\left(\frac{v}{\bar{q}}-\frac{P}{\bar{q}}\right)-\Phi^{(r)}(0)b_{r+1}\left(\frac{v}{\bar{q}}\right)\right)$$
$$-\int_0^{P/\bar{q}}\Phi^{(l)}(x)b_l\left(\frac{v}{\bar{q}}-x\right)\mathrm{d}x.$$

由

$$\int_0^{P/\bar{q}}\Phi(x)\mathrm{d}x=\int_0^{P/\bar{q}}e(\beta f(\bar{q}x))\mathrm{d}x=\frac{1}{\bar{q}}\int_0^P e(\beta f(y))\mathrm{d}y,$$

可知

$$T(\alpha)=T^*(\alpha,h,q)+\sum_{r=1}^{l-1}\left(\Phi^{(r)}\left(\frac{P}{\bar{q}}\right)a_{r+1}\left(\frac{P}{\bar{q}}\right)-\Phi^{(r)}(0)a_{r+1}(0)\right)-R,$$

此处

$$a_{r+1}(t)=\sum_{v=1}^{\bar{q}}e_q(hf(v))b_{r+1}\left(\frac{v}{\bar{q}}-t\right)$$

及

$$R=\sum_{v=1}^{\bar{q}}e_q(hf(v))\int_0^{P/\bar{q}}\Phi^{(l)}(x)b_l\left(\frac{v}{\bar{q}}-x\right)\mathrm{d}x.$$

现在取 $l=\left[\frac{1}{\varepsilon}\right]+1$, 则由引理 7.8, 可知

$$\Phi^{(l)}(x)\ll P^{-1}$$

及

$$R\ll\bar{q}\int_0^{P/\bar{q}}P^{-1}\mathrm{d}x\ll 1.$$

命

$$s_v = \sum_{x=1}^{v} e_q(hf(x)).$$

$$\begin{aligned} a_{r+1}(t) =& s_1 b_{r+1}\left(\frac{1}{\bar{q}} - t\right) + \sum_{v=2}^{\bar{q}-1}(s_v - s_{v-1}) b_{r+1}\left(\frac{v}{\bar{q}} - t\right) \\ =& \sum_{m=1}^{\bar{q}-1} s_m \left(b_{r+1}\left(\frac{m}{\bar{q}} - t\right) - b_{r+1}\left(\frac{m+1}{\bar{q}} - t\right)\right) + s_{\bar{q}} b_{r+1}(1-t). \end{aligned}$$

由定理 2,

$$s_v = O(q^{1-a+\varepsilon}).$$

因 $b_{r+1}(x)$ 是一囿变函数, 故得

$$\begin{aligned} |a_{r+1}(t)| \ll & q^{1-a+\varepsilon}\left(\sum_{m=1}^{\bar{q}-1}\left|b_{r+1}\left(\frac{m}{q} - t\right) - b_{r+1}\left(\frac{m+1}{\bar{q}} - t\right)\right| + 1\right) \\ \ll & q^{1-a+\varepsilon}. \end{aligned}$$

再用引理 7.8 即得

$$\begin{aligned} T(\alpha) - T^*(\alpha, h, q) \ll & \left(\sum_{r=1}^{l-1} P^{-r\varepsilon} + 1\right) q^{1-a+\varepsilon} \\ \ll & q^{1-a+\varepsilon}. \end{aligned}$$

§7.6 估计展开在 $\mathfrak{M}(h,q)$ 上的积分之数值

引理 7.12 当 $2t > 2k+1$ 时,

$$\sum_{\mathfrak{M}} \int_{\mathfrak{M}} |T(\alpha)|^{2t} \mathrm{d}\alpha \ll P^{2t-k}.$$

证 由引理 7.10 及 7.11, 可知在 $\mathfrak{M}(h,q)$ 上

$$\begin{aligned} T(\alpha) \ll & q^{-a+\varepsilon} \min(P, |\beta|^{-a}) + q^{1-a+\varepsilon} \\ \ll & q^{-a+\varepsilon} \min(P, |\beta|^{-a}). \end{aligned}$$

引理中所述及的和不超过

$$\ll \sum_{\mathfrak{M}} \int_{\mathfrak{M}} q^{-2ta+\varepsilon} \min(P^{2t}|\beta|^{-2ta}) \mathrm{d}\beta$$

$$\ll \sum_{q\leqslant P^{1-\varepsilon}}\sum_{h=1}^{q} q^{-2ta+\varepsilon}\left(\int_0^{P-k} P^{2t}\mathrm{d}\beta+\int_{p-k}\beta^{-2ta}\mathrm{d}\beta\right)$$
$$\ll P^{2t-k}\sum_{q\leqslant P^{1-\varepsilon}} q^{1-2ta+\varepsilon}\ll P^{2t-k}$$

(由于 $\sum q^{1-2ta}$ 的收敛性).

引理 7.13 当 $k\geqslant 12$ 及

$$t>k^2(2\log k+\log\log k+2.5)-2$$

时,

$$r_{2t}(P)\ll P^{2t-k}.$$

这是由引理 7.9 及 7.12 直接推出的结果.

§7.7 证明定理所必需的引理

命 $N=f(P)$,

$$\mathfrak{T}(\alpha)=\sum_{p\leqslant P} e(f(p)\alpha),$$
$$\mathfrak{T}^*(\alpha,h,q)=\frac{1}{A^a}\frac{W_{h,q}}{\varphi(\bar{q})}\sum_{2\leqslant n\leqslant N}\frac{e(n\beta)}{n^{1-a}\log\dfrac{n}{A}},$$

此处 A 是 $f(x)$ 的最高方次的系数, $W_{h,q}$ 的定义见本章之首.

我们仍如 §3 来分割隔间 $-\dfrac{1}{\tau}\leqslant\alpha\leqslant 1-\dfrac{1}{\tau}$, 但现在却用 $q\leqslant\tau=NL^{-\sigma}$, 此处我们选择了 σ 使定理 10 中的 σ_0 大于定理 4 中的 $c_2(k,k)$ 加上某一整数 s_1.

用 $\mathfrak{M}(h,q)$ 代表隔间

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{1}{q\tau},\quad q\leqslant L^{\sigma}.$$

用 E 代表隔间 $\left(-\dfrac{1}{\tau},1-\dfrac{1}{\tau}\right)$ 中所有不在 $\mathfrak{M}(h,q)$ 内的点. 容易证明 (如前) 所有的 $\mathfrak{M}(h,q)$ 无公共点.

引理 7.14 (Siegel-Walfisz)* 假定 $q\leqslant L^{\sigma},(l,q)=1,n\leqslant P$. 命 $\pi(n;l,q)$ 代表算术级数 $l+qx$ 中不大于 n 的素数的个数. 则

$$\pi(n;l,q)=\frac{1}{\varphi(q)}\mathrm{li}n+O(P\mathrm{e}^{-c_1\sqrt{L}}),$$

**Math.Zs.*, 40(1936), 529—601, Hilfsatz 3. 关于完整的证明, 可参考: Н.Г Чудаков, введение вгеориЮ L-функций дирихле, 或 T. Estermann, Introduction to modern prime number theory.

此处 $\mathrm{li}\, x = \int_2^x \frac{\mathrm{d}t}{\log t}$, 符号 O 所包含的常数与 q 无关.

引理 7.15 在 $\mathfrak{M}(h,q)$ 上,

$$\mathfrak{T}(\alpha) - \mathfrak{T}^*(\alpha, h, q) = O(P\mathrm{e}^{-c_2\sqrt{L}}).$$

证 命 $\alpha = \frac{h}{q} + \beta$. 又命

$$S_n = \sum_{f(p) \leqslant n} e_q(hf(p)), \quad n \leqslant N,$$

则

$$S_n = \sum_{\substack{l=1 \\ (l,\bar{q})=1}}^{\bar{q}} e_q(hf(l))\pi(n'; l, \bar{q}) + O(q^\varepsilon),$$

此处 n' 是方程 $f(x) = n$ 的最大正根. (当 n 充分大时, n' 是一定存在的, 且是唯一的). 今往证明

$$n' - \left(\frac{n}{A}\right)^a \ll 1.$$

这是由于:

$$\begin{aligned} n' - \left(\frac{n}{A}\right)^a &= n' - \left(\frac{f(n')}{A}\right)^a = n' - ({n'}^k + O({n'}^{k-1}))^a \\ &= n'(1 - (1 + O({n'}^{-1}))^a) = O(1). \end{aligned}$$

由引理 7.14, 对充分大的 n 我们有

$$\begin{aligned} \pi(n'; l, \bar{q}) &= \frac{1}{\varphi(\bar{q})} \mathrm{li} n' + O(P\mathrm{e}^{-c_1\sqrt{L}}) \\ &= \frac{1}{\varphi(\bar{q})} \mathrm{li} \left(\frac{n}{A}\right)^a + O(P\mathrm{e}^{-c_1\sqrt{L}}). \end{aligned}$$

最后的等式对所有的不大于 P 的数 n' 都真实. 由此得出

$$\begin{aligned} S_n &= \sum_{\substack{l=1 \\ (l,\bar{q})=1}}^{\bar{q}} e_q(hf(l)) \left(\frac{1}{\varphi(\bar{q})} \mathrm{li} \left(\frac{n}{A}\right)^a + O(P\mathrm{e}^{-c_1\sqrt{L}})\right) + O(q^\varepsilon) \\ &= \sum_{\substack{l=1 \\ (l,\bar{q})=1}}^{\bar{q}} \frac{e_q(hf(l))}{\varphi(\bar{q})} \mathrm{li} \left(\frac{n}{A}\right)^a + O(P\mathrm{e}^{-c_3\sqrt{L}}) \\ &= \frac{W_{h,q}}{\varphi(\bar{q})} \mathrm{li} \left(\frac{n}{A}\right)^a + O(P\mathrm{e}^{-c_3\sqrt{L}}). \end{aligned}$$

因此

$$\begin{aligned}\mathfrak{T}(\alpha) &= \sum_{n=2}^{N}(S_n - S_{n-1})e(n\beta) + O(1)\\ &= \sum_{n=2}^{N} S_n(e(n\beta) - e((n+1)\beta)) + S_N e((N+1)\beta) + O(1)\\ &= \frac{W_{h,q}}{\varphi(\bar{q})}\left(\sum_{n=2}^{N}\mathrm{li}\left(\frac{n}{A}\right)^a (e(n\beta) - e((n+1)\beta))\right.\\ &\quad \left. + \mathrm{li}\left(\frac{N}{A}\right)^a e((N+1)\beta)\right) + O(P\mathrm{e}^{-c_4\sqrt{L}}).\end{aligned}$$

由于

$$\begin{aligned}\mathrm{li}\left(\frac{n}{A}\right)^a - \mathrm{li}\left(\frac{n-1}{A}\right)^a &= \int_{((n-1)/A)^a}^{(n/A)^a}\frac{\mathrm{d}t}{\log t}\\ &= A^{-a}\int_{(n-1)^a}^{n^a}\frac{\mathrm{d}y}{\log(yA^{-a})} = \frac{1}{A^a n^{1-a}\log\dfrac{n}{A}} + O\left(\frac{1}{n^{2-a}\log n}\right),\end{aligned}$$

因而得出所需要的结果.

引理 7.16　当 $|\beta| \leqslant \dfrac{1}{2}$ 时,

$$\mathfrak{T}^*(\alpha, h, q) \ll q^{-a+\varepsilon}\min(P, |\beta|^{-a}).$$

在 $\mathfrak{M}(h,q)$ 上对于 $\mathfrak{T}(\alpha)$ 也有类似的结果.

证　由定理 1 的推理 1.3 可得

$$\begin{aligned}\mathfrak{T}^*(\alpha, h, q) &\ll q^{-a+\varepsilon}\sum_{n\leqslant f(P)}\frac{1}{n^{1-a}}\\ &\ll q^{-a+\varepsilon}P.\end{aligned}$$

(此处用了 $\varphi(q) \gg \dfrac{q}{d(q)} \gg q^{1-\varepsilon}$). 又

$$\sum_{n\leqslant N}\frac{e(n\beta)}{n^{1-a}\log\dfrac{n}{A}} = \sum_{n\leqslant|\beta|^{-1}}\frac{e(n\beta)}{n^{1-a}\log\dfrac{n}{A}} + \sum_{N\geqslant n>|\beta|^{-1}}\frac{e(n\beta)}{n^{1-a}\log\dfrac{n}{A}}.$$

以 $\sum_1$ 及 $\sum_2$ 分别表示这两个和, 显然有

$$\left|\sum\nolimits_1\right| \ll \sum_{n\leqslant|\beta|^{-1}}\frac{1}{n^{1-a}\log n} = O(|\beta|^{-a}).$$

命 $S_n = \sum_{|\beta|-1<m<n} e(m\beta)$, 由分部求和法可得

$$\left|\sum\nolimits_2\right| = \left|\sum_{N\geqslant n>|\beta|^{-1}} \frac{e(n\beta)}{n^{1-a}\log\frac{n}{A}}\right| = \left|\sum_{N\geqslant n>|\beta|^{-1}} \frac{S_n - S_{n-1}}{n^{1-a}\log\frac{n}{A}}\right|$$

$$\leqslant \sum_{N\geqslant n>|\beta|^{-1}} |S_n| \left(\frac{1}{n^{1-a}\log\frac{n}{A}} - \frac{1}{(n+1)^{1-a}\log\left(\frac{n+1}{A}\right)}\right)$$

$$+ \frac{|S_N|}{(N+1)^{1-a}\log\frac{N+1}{A}}.$$

因为 $|S_n| \leqslant \frac{1}{|\beta|}$, 可知

$$\left|\sum\nolimits_2\right| \leqslant \sum_{N\geqslant n>|\beta|^{-1}} \frac{1}{|\beta|} \left(\frac{1}{n^{1-a}\log\frac{n}{A}} - \frac{1}{(n+1)^{1-a}\log\left(\frac{n+1}{A}\right)}\right)$$

$$+ \frac{1}{|\beta|}\frac{1}{(N+1)^{1-a}\log\frac{N+1}{A}} \ll |\beta|^{-a}.$$

这证明了引理中的第一个结论.

由引理 7.15, 可知

$$\mathfrak{T}(\alpha) = \mathfrak{T}^*(\alpha, h, q) + O(P\mathrm{e}^{-c_2\sqrt{L}}).$$

因为 $P\mathrm{e}^{-c_2\sqrt{L}} \ll Pq^{-a}$ 及 $P\mathrm{e}^{-c_2\sqrt{L}} \ll |\beta|^{-a}q^{-a}$, 可得

$$\mathfrak{T}(\alpha) \ll q^{-a+\varepsilon}\min(P, |\beta|^{-a}).$$

§7.8　定理的证明

我们先证明一个与定理 11 略有不同的定理.

定理 11′　假定

$$s \geqslant \begin{cases} 2^k + 1, & \text{当} 1 \leqslant k \leqslant 11, \\ 2k^2(2\log k + \log\log k + 2.5), & \text{当} k > 11, \end{cases}$$

则对任一已给的整数 s_1, 常有

$$\left|I_s(N) - A^{-sa}\mathfrak{S}(N)\Psi(N)\right| \leqslant \frac{c(k, s_1, f(x)\text{的系数})N^{sa-1}}{(\log N)^{s_1}},$$

此处

$$\Psi(N)=\sum_{\substack{n_1+\cdots+n_s=N\\ n_v\geqslant 2}}\frac{1}{n_1^{1-a}\log\frac{n_1}{A}\cdots n_s^{1-a}\log\frac{n_s}{A}}.$$

证　1) 我们有

$$\begin{aligned}I_s(N)&=\int_0^1\mathfrak{T}^s(\alpha)e(-N\alpha)\mathrm{d}\alpha=\int_{-\frac{1}{\tau}}^{1-\frac{1}{\tau}}\mathfrak{T}^s(\alpha)e(-N\alpha)\mathrm{d}\alpha\\&=\int_E\mathfrak{T}^s(\alpha)e(-N\alpha)\mathrm{d}\alpha+\sum_{\mathfrak{M}(h,q)}\int_{\mathfrak{M}(h,q)}\mathfrak{T}^s(\alpha)e(-N\alpha)\mathrm{d}\alpha.\end{aligned}$$

2) 当 $k>11$. 由于 $s>2k^2(2\log k+\log\log k+2.5)$, 我们可以选择整数 t, 使

$$s-2t\geqslant 1,\quad t>k^2(2\log k+\log\log k+2.5)-2.$$

由定理 10 及引理 7.13, 可得

$$\begin{aligned}\int_E\mathfrak{T}^s(\alpha)e(-N\alpha)\mathrm{d}a\ll&(PL^{-\sigma_0})^{s-2t}\int_0^1|\mathfrak{T}(\alpha)|^{2t}\mathrm{d}\alpha\\\ll&P^{s-2t}L^{-s_1}\int_0^1|T(\alpha)|^{2t}\mathrm{d}\alpha\\\ll&P^{s-k}L^{-s_1}.\end{aligned}$$

当 $1\leqslant k\leqslant 11$ 时, 由定理 4 可得

$$\begin{aligned}\int_E(\mathfrak{T}(\alpha))^{2^k+1}e(-N\alpha)\mathrm{d}\alpha\ll&PL^{-s_1-c_2(k,k)}\int_0^1|T(\alpha)|^{2k}\mathrm{d}\alpha\\\ll&P^{2^k-k+1}L^{-s_1}\end{aligned}$$

(由于 σ 的选择).

3) 由引理 7.15,7.16 及简单的不等式

$$|\xi^s-\eta^s|\leqslant s|\xi-\eta|\max(|\xi|^{s-1},|\eta|^{s-1}),$$

在 $\mathfrak{M}(h,q)$ 上我们有下面的结果:

$$\begin{aligned}|\mathfrak{T}^s(\alpha)-\mathfrak{T}^{*s}(\alpha,h,q)|\leqslant&s|\mathfrak{T}(\alpha)-\mathfrak{T}^*(\alpha,h,q)|\max(|\mathfrak{T}(\alpha)|^{s-1},|\mathfrak{T}^*(\alpha,h,q)|^{s-1})\\\ll&P\mathrm{e}^{-c_2\sqrt{L}}(q^{-a+\varepsilon})^{s-1}\min(P,|\beta|^{-a})^{s-1}.\end{aligned}$$

在 $\mathfrak{M}(h,q)$ 上求积分, 即得

$$\int_{\mathfrak{M}(h,q)}\mathfrak{T}^s(\alpha)e(-N\alpha)\mathrm{d}\alpha-\int_{\mathfrak{M}(h,q)}\mathfrak{T}^{*s}(\alpha,h,q)e(-N\alpha)\mathrm{d}\alpha$$

$$\ll P\mathrm{e}^{-c_2\sqrt{L}}q^{-a(s-1)+\varepsilon}\left(\int_0^{P-k}P^{s-1}\mathrm{d}\beta+\int_{P-k}\beta^{-a(s-1)}\mathrm{d}\beta\right)$$
$$\ll q^{-a(s-1)+\varepsilon}P^{s-k}\mathrm{e}^{-c_2\sqrt{L}}.$$

对所有的 $\mathfrak{M}(h,q)$ 求和, 得出

$$\sum_{\mathfrak{M}}\int_{\mathfrak{M}}\mathfrak{T}^s(\alpha)e(-N\alpha)\mathrm{d}\alpha-\sum_{\mathfrak{M}}\int_{\mathfrak{M}}\mathfrak{T}^{*s}(\alpha,h,q)e(-N\alpha)\mathrm{d}\alpha$$
$$\ll P^{s-k}\mathrm{e}^{-c_2\sqrt{L}}\sum_{q\leqslant L^\sigma}q^{1-a(s-1)+\varepsilon}$$
$$\ll P^{s-k}\mathrm{e}^{-c_5\sqrt{L}}.$$

4) 由引理 7.16, 我们有

$$\int_{\mathfrak{M}(h,q)}\mathfrak{T}^{*s}(\alpha,h,q)e(-N\alpha)\mathrm{d}\alpha-\int_{-\frac{1}{2}}^{\frac{1}{2}}\mathfrak{T}^{*s}(\alpha,h,q)e(-N\alpha)\mathrm{d}\beta$$
$$\ll q^{-as+\varepsilon}\int_{q^{-1}\tau^{-1}}^{\infty}\beta^{-as}\mathrm{d}\beta$$
$$\ll q^{-1+\varepsilon}P^{s-k}L^{-\sigma(sa-1)}.$$

故

$$\sum_{\mathfrak{M}}\int_{\mathfrak{M}}\mathfrak{T}^{*s}(\alpha,h,q)e(-N\alpha)\mathrm{d}\alpha-\sum_{\mathfrak{M}}\int_{-\frac{1}{2}}^{\frac{1}{2}}\mathfrak{T}^{*s}(\alpha,h,q)e(-N\alpha)\mathrm{d}\beta$$
$$\ll P^{s-k}L^{-\sigma(sa-1)}\sum_{q\leqslant L^\sigma}q^{\varepsilon}$$
$$\ll P^{s-k}L^{-\sigma(sa-2)+\varepsilon}\ll P^{s-k}L^{-s_1}.$$

(由于 $2s_1<\sigma$ 及 $sa-2\geqslant\dfrac{1}{2}$).

5) 我们有

$$\sum_{\mathfrak{M}}\int_{-\frac{1}{2}}^{\frac{1}{2}}\mathfrak{T}^{*s}(\alpha,h,q)e(-N\alpha)d\beta$$
$$=A^{-sa}\sum_{\mathfrak{M}}\left(\frac{W_{h,q}}{\varphi(\bar{q})}\right)^s e\left(-\frac{Nh}{q}\right)\int_{-\frac{1}{2}}^{\frac{1}{2}}\left(\sum_{2\leqslant n\leqslant N}\frac{e(n\beta)}{n^{1-a}\log\dfrac{n}{A}}\right)^s e(-N\beta)\mathrm{d}\beta$$
$$=A^{-sa}\sum_{q\leqslant L^\sigma}\sum_{\substack{h=1\\(h,q)=1}}^{q}\left(\frac{W_{h,q}}{\varphi(\bar{q})}\right)^s e\left(-\frac{Nh}{q}\right)\Psi(N),$$

此处 $\Psi(N)$ 之定义见定理 11′.

6) 我们有

$$\left|\sum_{q>l^\sigma}\sum_{\substack{h=1\\(h,q)=1}}^{\bar q}\left(\frac{W_{h,q}}{\varphi(\bar q)}\right)^s e\left(-\frac{Nh}{q}\right)\right| \ll \sum_{q>L^\sigma} q\cdot q^{-sa+\varepsilon} \ll L^{(2-sa)\sigma+\varepsilon} \ll L^{-s_1}.$$

故

$$\sum_{q\leqslant L^\sigma}\sum_{\substack{h=1\\(h,q)=1}}\left(\frac{W_{h,q}}{\varphi(\bar q)}\right)^s e\left(-\frac{Nh}{q}\right) = \mathfrak{S}(N)+O(L^{-s_1}).$$

7) 总结 3), 4), 5) 及 6) 的结果, 我们得出

$$\sum_{\mathfrak{M}(h,q)}\int_{\mathfrak{M}(h,q)} \mathfrak{T}^s(\alpha)e(-N\alpha)\mathrm{d}\alpha = \mathfrak{S}(N)A^{-sa}\Psi(N)+O(N^{sa-1}L^{-s_1}).$$

再由 1) 及 2) 的结果可知

$$I_s(N) = \mathfrak{S}(N)A^{-sa}\Psi(N)+O(N^{sa-1}L^{-s_1}).$$

§7.9　定理 11 的证明

引理 7.17　当 $0<\lambda_1<1$ 及 $\lambda_2\geqslant\lambda_1$ 时,

$$\sum_{n=1}^{N-1}\frac{1}{n^{1-\lambda_1}(N-n)^{1-\lambda_2}} = \frac{\Gamma(\lambda_1)\Gamma(\lambda_2)}{\Gamma(\lambda_1+\lambda_2)}N^{\lambda_1+\lambda_2-1}(1+O(N^{-\lambda_1})).$$

证　写

$$\sum_{n=1}^{N-1}\frac{1}{n^{1-\lambda_1}(N-n)^{1-\lambda_2}} = N^{\lambda_1+\lambda_2-1}\sum_{n=1}^{N-1}\frac{\frac{1}{N}}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}.$$

对 $\dfrac{n}{N}\leqslant x\leqslant\dfrac{n+1}{N}$, 命 $x=\dfrac{n}{N}+\dfrac{\theta}{N}(0\leqslant\theta\leqslant 1)$, 则得

$$\begin{aligned}&\frac{1}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}-\frac{1}{x^{1-\lambda_1}(1-x)^{1-\lambda_2}}\\ =&\frac{1}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}\left(1-\left(1+\frac{\theta}{n}\right)^{\lambda_1-1}\left(1-\frac{\theta}{N-n}\right)^{\lambda_2-1}\right)\end{aligned}$$

$$=\frac{1}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}\left(O\left(\frac{1}{n}\right)+O\left(\frac{1}{N-n}\right)\right).$$

因此

$$\begin{aligned}&\sum_{n=1}^{N-1}\frac{1}{n^{1-\lambda_1}(N-n)^{1-\lambda_2}}\\&=N^{\lambda_1+\lambda_2-1}\Bigg(\int_0^1 x^{\lambda_1-1}(1-x)^{\lambda_2-1}\mathrm{d}x\\&\quad+O\Bigg(\sum_{n=1}^{N-1}\frac{\frac{1}{nN}}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}+\sum_{n=1}^{N-1}\frac{\frac{1}{(N-n)N}}{\left(\frac{n}{N}\right)^{1-\lambda_1}\left(1-\frac{n}{N}\right)^{1-\lambda_2}}\Bigg)\Bigg)\\&=N^{\lambda_1+\lambda_2-1}\frac{\Gamma(\lambda_1)\Gamma(\lambda_2)}{\Gamma(\lambda_1+\lambda_2)}+O\Bigg(\sum_{n=1}^{N-1}\frac{1}{n^{2-\lambda_1}(N-n)^{1-\lambda_2}}\\&\quad+\sum_{n=1}^{N-1}\frac{1}{n^{1-\lambda_1}(N-n)^{2-\lambda_2}}\Bigg).\end{aligned}$$

因为

$$\begin{aligned}\sum_{n=1}^{N-1}\frac{1}{n^{2-\lambda_1}(N-n)^{1-\lambda_2}}&=\sum_{n\leqslant\frac{1}{2}N}\frac{1}{n^{2-\lambda_1}(N-n)^{1-\lambda_2}}+\sum_{N>n>\frac{1}{2}N}\frac{1}{n^{2-\lambda_1}(N-n)^{1-\lambda_2}}\\&\ll N^{\lambda_2-1}\sum_{n\leqslant\frac{1}{2}N}\frac{1}{n^{2-\lambda_1}}+N^{\lambda_1-2}\sum_{N>n>\frac{1}{2}N}\frac{1}{(N-n)^{1-\lambda_2}}\\&\ll N^{\lambda_2-1}\end{aligned}$$

及

$$\sum_{n=1}^{N-1}\frac{1}{n^{1-\lambda_1}(N-n)^{2-\lambda_2}}\ll N^{\lambda_1+\lambda_2-1-\min(1,\lambda_2)}\begin{cases}1, & \text{若}\lambda_2\neq 1,\\ \log N, & \text{若}\lambda_2=1,\end{cases}$$

即得出本引理.

引理 7.18

$$\sum_{\substack{n_1+\cdots+n_s=N\\ n_\nu>0}}\frac{1}{n_1^{1-a}\cdots n_s^{1-a}}=\frac{\Gamma^s(a)}{\Gamma(sa)}N^{sa-1}(1+O(N^{-a})).$$

证 由引理 7.17 已知此引理当 $s=2$ 时真实. 今假定引理对 $s-1$ 真实而运用归纳法. 由引理 7.17 可知

$$\sum_{\substack{n_1+\cdots+n_s=N\\ n_\nu>0}}\frac{1}{n_1^{1-a}\cdots n_s^{1-a}}=\sum_{n_1=1}^{N-s+1}\frac{1}{n_1^{1-a}}\sum_{n_2+\cdots+n_s=N-n_1}\frac{1}{n_2^{1-a}\cdots n_s^{1-a}}$$

$$=\sum_{n_1}\frac{1}{n_1^{1-a}}\frac{\Gamma^{s-1}(a)}{\Gamma((s-1)a)}(N-n_1)^{(s-1)a-1}+O\left(\sum_{n_1}\frac{1}{n_1^{1-a}(N-n)^{1-(s-2)a}}\right)$$
$$=\frac{\Gamma^s(a)}{\Gamma(sa)}N^{sa-1}(1+O(N^{-a})).$$

引理 7.19

$$\sum_{\substack{n_1+\cdots+n_s=N\\ n_v>1}}\frac{1}{n_1^{1-a}\log\frac{n_1}{A}\cdots n_s^{1-a}\log\frac{n_s}{A}}=\frac{\Gamma^s(a)}{\Gamma(sa)}\frac{N^{sa-1}}{\log^s N}\left(1+O\left(\frac{\log L}{L}\right)\right).$$

证　命

$$\Psi_0(N)=\sum_{\substack{n_1+\cdots+n_s=N\\ n_v>1}}\frac{1}{n_1^{1-a}\cdots n_s^{1-a}},$$

$$\Psi_\mu(N)=\sum_{\substack{n_1+\cdots n_s=N\\ n_v>1}}\frac{1}{n_1^{1-a}\log\frac{n_1}{A}\cdots n_\mu^{1-a}\log\frac{n_\mu}{A}\cdot n_{\mu+1}^{1-a}\cdots n_s^{1-a}},\quad 0<\mu\leqslant s,$$

则

$$\Psi_\mu(N)=\frac{1}{L}\Psi_{\mu-1}(N)+O\left(\frac{\Psi_\mu(N)\log L}{L}\right)+O\left(\frac{N^{sa-1}}{L^{s+1}}\right).\tag{1}$$

此式的证明如下：分和为两部分

$$\Psi_\mu(N)=\sum_{n_\mu\leqslant NL^{-\delta}}+\sum_{n_\mu>NL^{-\delta}}=S_1+S_2,$$

则

$$S_1\ll\sum_{\substack{n_1+\cdots+n_s=N\\ n_\mu\leqslant NL^{-\delta}}}\frac{1}{n_1^{1-a}\cdots n_s^{1-a}}$$
$$\ll\sum_{n_\mu\leqslant NL^{-\delta}}\frac{1}{n_\mu^{1-a}}\sum_{n_1+\cdots+n_{\mu-1}+n_{\mu+1}+\cdots+n_s=N-n_\mu}\frac{1}{n_1^{1-a}\cdots n_{\mu-1}^{1-a}n_{\mu+1}^{1-a}\cdots n_s^{1-a}}$$
$$\ll\sum_{n_\mu\leqslant NL^{-\delta}}\frac{1}{n_\mu^{1-a}}(N-n_\mu)^{(s-1)a-1}$$
$$\ll N^{(s-1)a-1}(NL^{-\delta})^a=N^{sa-1}L^{-\delta a}\ll N^{sa-1}L^{-s-1}.$$

此处取 $\delta=k(s+1)$. 又

$$S_2=\frac{1}{\log N}\sum_{\substack{n_1+\cdots+n_s=N\\ n_\mu>NL^{-\delta}}}\frac{1}{n_1^{1-a}\log\frac{n_1}{A}\cdots n_{\mu-1}^{1-a}\log\frac{n_{\mu-1}}{A}\cdot n_\mu^{1-a}\cdots n_s^{1-a}}$$

$$
\begin{aligned}
&+\sum \frac{1}{n_1^{1-a}\log\frac{n_1}{A}\cdots n_\mu^{1-a}\cdots n_s^{1-a}}\left(\frac{1}{\log\frac{n_\mu}{A}}-\frac{1}{\log N}\right)\\
=&\frac{1}{\log N}\Psi_{\mu-1}(N)+O\left(\frac{N^{sa-1}}{L^{s+1}}\right)+O\left(\frac{\log L}{L}\Psi_\mu(N)\right).
\end{aligned}
$$

这证明了 (1) 式.

由 (1) 式可知

$$
\Psi_\mu(N)=\frac{1}{\log N}\Psi_{\mu-1}(N)+O\left(\frac{\Psi_{\mu-1}(N)\log L}{L^2}\right)+O\left(\frac{N^{sa-1}}{L^{s+1}}\right),
$$

续用多次可以推得

$$
\begin{aligned}
\Psi_s(N)=&\frac{1}{\log^s N}\Psi_0(N)+O\left(\frac{\Psi_0(N)\log L}{L^{s+1}}\right)+O\left(\frac{N^{sa-1}}{L^{s+1}}\right)\\
=&\frac{1}{\log^s N}\Psi_0(N)+O\left(\frac{N^{sa-1}}{L^{s+1}}\log L\right).
\end{aligned}
$$

由引理 7.18 得出本引理.

由定理 11′ 及引理 7.19 可以得出本章开始所宣称的定理 (定理 11).

第8章 奇异级数

§8.1

今研究 $f(x)=x^k$ 时奇异级数的性质.

命 $p^\theta\|k$,

$$\gamma=\begin{cases}\theta+2, & 若p=2,2|k,\\ \theta+1, & 其他的情况\end{cases}$$

及

$$K=\prod_{(p-1)|k}p^\gamma.$$

定理 12 假定 $s\geqslant 3k+1$ 及对所有适合 $(p-1)|k$ 的 p, 常有 $s\equiv N(\bmod p^\gamma)$. 并取 $f(x)=x^k$. 则 $\mathfrak{S}(N)\geqslant A>0$, 此处 A 并不依于 N.

§8.2 关于三角和的引理

引理 8.1 若 $(q_1,q_2)=1$, 则

$$W_{h,q_1q_2}=W_{hq_1^{k-1},q_2}W_{hq_2^{k-1},q_1}$$

及

$$B_s(N,q_1q_2)=B_s(N,q_1)B_s(N,q_2).$$

证 命 $l=l_1q_2+l_2q_1$, 则

$$W_{h,q_1q_2}=\sum_{\substack{q_1=1\\(l_1,q_1)=1}}^{q_1}\sum_{\substack{l_2=1\\(l_2,q_2)=1}}^{q_2}e_{q_1q_2}(hq_2^kl_1^k+hq_1^kl_2^k)=W_{hq_1^{k-1},q_2}W_{hq_2^{k-1},q_1}.$$

又命 $h=h_1q_2+h_2q_1$, 则

$$\begin{aligned}B_s(N,q_1,q_2)&=\sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1}\sum_{\substack{h_2=1\\(h_2,q_2)=1}}^{q_2}\left(\frac{W_{h_2q_1^k,q_2}}{\varphi(q_2)}\right)^s\left(\frac{W_{h_1q_2^k,q_1}}{\varphi(q_1)}\right)^se_{q_1}(-h_1N)e_{q_2}(-h_2N)\\&=\sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1}\sum_{\substack{h_2=1\\(h_2,q_2)=1}}^{q_2}\left(\frac{W_{h_2,q_2}}{\varphi(q_2)}\right)^s\left(\frac{W_{h_1,q_1}}{\varphi(q_1)}\right)^se_{q_1}(-h_1N)e_{q_2}(-h_2N)\\&=B_s(N,q_1)B_s(N,q_2).\end{aligned}$$

引理 8.2 命

$$\mu \geqslant \begin{cases} 1, & 若p > 2, \\ 2, & 若p = 2. \end{cases}$$

若

$$x \equiv y + zp^{\mu}. \quad (\bmod\ p^{\mu+1}),$$

则

$$x^p \equiv y^p + y^{p-1}zp^{\mu+1} \quad (\bmod p^{\mu+2}).$$

证 写

$$x = y + zp^{\mu} + mp^{\mu+1}.$$

由 $3\mu \geqslant \mu + 2$, 可知

$$x^p \equiv (y + zp^{\mu})^p \equiv y^p + y^{p-1}zp^{\mu+1} + \frac{1}{2}(p-1)py^{p-2}z^2p^{2\mu}(\bmod p^{\mu+2}).$$

若 $p > 2$, 则有

$$\frac{1}{2}(p-1)py^{p-2}z^2p^{2\mu} \equiv 0 \quad (\bmod p^{\mu+2}).$$

当 $p = 2$, 由 $\mu \geqslant 2, 2\mu \geqslant \mu + 2$. 故

$$\frac{1}{2}p(p-1)y^{p-2}z^2p^{2\mu} \equiv 0 \quad (\bmod p^{\mu+2}).$$

从此二式可以得出本引理.

引理 8.3 若 $t > \gamma$ 及 $p \nmid h$, 则

$$W_{h,p^t} = 0.$$

证 命 $l = l_1 + l_2p^{t-\theta-1}$, 则由重复运用引理 8.2 可得

$$l^{p^{\theta}} \equiv l_1^{p^{\theta}} + l_1^{p^{\theta}-1}l_2p^{t-1} \quad (\bmod p^t).$$

于是

$$l^k \equiv l_1^k + kl_1^{k-1}l_2p^{t-\theta-1} \quad (\bmod p^t).$$

由此推得

$$W_{h,p^t} = \sum_{\substack{l_1=1 \\ (l_1,p)=1}}^{p^{t-\theta-1}} \sum_{l_2=1}^{p^{\theta+1}} e_{p^t}\left(h(l_1^k + p^{t-\theta-1}kl_1^{k-1}l_2)\right) = 0.$$

(由于 $p \nmid l_1kp^{-\theta}$).

引理 8.4　同余式

$$x^k \equiv a(\text{mod}p), \quad p \nmid a,$$

或无解, 或有 $(k, p-1)$ 个解. 当 x 经过 $1, 2\cdots, p-1(\text{mod}p)$ 时, x^k 经过 $(p-1)/(k, p-1)$ 个互不同余的数, mod$p$.

证　同余式 $x^k \equiv 1(\text{mod}p)$ 有 $(p-1, k)$ 个解. 此点可由 $x^{p-1} \equiv 1(\text{mod}p)$ 推得之. 又命

$$a_1 \cdots, a_{(k,p-1)}$$

表其诸解. 若 $x_1^k \equiv a(\text{mod}p)$, 则

$$x_1 a_1, \cdots, x_1 a_{(k,p-1)}$$

都是 $x^k \equiv a(\text{mod}p)$ 的解, 且无他解. 所以同余式

$$x^k \equiv a(\text{mod}p), \quad p \nmid a,$$

或无解, 或有 $(k, p-1)$ 个解. 因之得出本引理.

引理 8.5　若 $(h, q) = 1$, 则

$$|W_{h,q}| \leqslant c_1(k, \varepsilon) q^{1/2+\varepsilon}.$$

证　1) 证 q 是一素数 p. 则由引理 8.4 可知

$$\frac{1}{p}\sum_{h=1}^{p}\left|\sum_{x=1}^{p} e_p(hx^k)\right|^2 = \sum_{x^k \equiv y^k}\sum_{(\text{mod}p)} 1 = (k, p-1)(p-1) + 1.$$

考察和

$$\sum_{x=1}^{p} e_p(hx^k) = \sum_{x=1}^{p} e_p(h(\lambda x)^k) = \sum_{x=1}^{p} e_p(h\lambda^k x^k), \quad \lambda = 1, \cdots, p-1.$$

由于 λ^k 经过 $(p-1)/(k, p-1)$ 个互不相合的整数, mod p, 故

$$\begin{aligned}\frac{p-1}{(k, p-1)}\left|\sum_{x=1}^{p} e_p(hx^k)\right|^2 &\leqslant \sum_{h=1}^{p}\left|\sum_{x=1}^{p} e_p(hx^k)\right|^2 \\ &\leqslant ((k, p-1)(p-1) + 1)p.\end{aligned}$$

因之

$$\left|\sum_{x=1}^{p} e_p(hx^k)\right| \leqslant \sqrt{\frac{k^2 p^2}{p-1}} \leqslant 2k\sqrt{p},$$

即

$$|W_{h,p}| \leqslant 3k\sqrt{p}.$$

2) 若 $p|k$, 由引理 8.3 易见

$$W_{h,p^t} = O(1).$$

又由引理 8.3 可见当 $p \nmid k$ 及 $t > \gamma = \theta + 1 = 1$ 时也有

$$W_{h,p^t} = O(1).$$

由 1) 可知对所有的 p 常有

$$|W_{h,p}| \leqslant 3k\sqrt{p},$$

即当 $p \geqslant (3k)^{1/\varepsilon}$ 时,

$$|W_{h,p}| \leqslant p^{\frac{1}{2}+\varepsilon}.$$

命 $q = p_t^{l_1} \cdots p_t^{l_t}, p_1 < p_2 < \cdots < p_t$, 则由引理 8.1 可知

$$|W_{h,q}| = \prod_{p_i \leqslant k^{1/\varepsilon}} |W_{h_i,p^l i}| \prod_{p_i > k^{1/\varepsilon}} |W_{h_i,p^l i}| = O(q^{\frac{1}{2}+\varepsilon}).$$

§8.3　关于同余式的引理

引理 8.6　以 $M_s(p^t, N)$ 表同余式

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^t}, \quad p \nmid x_1 \cdots x_s,\ 0 < x_v < p^t$$

的解数. 则

$$\varphi(p^t)^{-s} p^t M_s(p^t, N) = 1 + \sum_{d=1}^{t} B_s(N, p^d).$$

证　有

$$\begin{aligned} M_s(p^t, N) =& p^{-t} \sum_{\substack{l_1=1 \\ p \nmid l_1}}^{p^t} \cdots \sum_{\substack{l_s=1 \\ p \nmid l_s}}^{p^t} \sum_{h=1}^{p^t} e_{p^t}(h(l_1^k + \cdots + l_s^k - N)) \\ =& p^{-t} \sum_{h=1}^{p^t} W_{h,p^t}^s e_{p^t} - hN = p^{-t} \varphi^s(p^t)(1 + \sum_{d=1}^{t} B_s(N, p^d)). \end{aligned}$$

引理 8.7　(Cauchy). 设 $x_1, x_2, \cdots, x_m$ 代表 m 个不同的剩余系 (mod p^l), $y_1, y_2, \cdots, y_n$ 代表 n 个不同的剩余系 (mod p^l), 且存在一数 y_i 使当 $i \neq j$ 时,

$y_i - y_j \not\equiv 0 (\bmod\, p)$, 则 $x_u + y_v (1 \leqslant u \leqslant m, 1 \leqslant v \leqslant n)$ 所代表的不同剩余系 $(\bmod\, p^l)$ 的数目

$$\geqslant \min(m+n-1, p^l).$$

证　当 $n=1$ 时, 引理显然成立. 设 $n \geqslant 2$, 并不妨假设 y_1 适合 $y_i \not\equiv y_1 (\bmod p)$ $(i \neq 1)$. 命 $z_1, \cdots, z_t$ 代表形如 $x_u + y_v$ 的不同剩余系 $(\bmod\, p^l)$. 若 $t = p^l$, 则引理已经成立, 故可设 $t < p^l$. 命 X, Y, Z 分别表示集合 $x_1, x_2, \cdots, x_m$; $y_1, y_2, \cdots, y_n$ 与 $z_1, z_2, \cdots, z_t$.

因 $p \nmid y_n - y_1$, 故当 λ 经过 $\lambda = 0, 1, \cdots, p^l - 1$ 时. $x_1 + y_1 + \lambda(y_n - y_1)$ 通过模 p^l 的一完全剩余系, 故它所表示之数必有不属于 Z 者. 命 λ_0 为最小的 $\lambda (0 \leqslant \lambda \leqslant p^l - 1)$ 使 $x_1 + y_1 + \lambda(y_n - y_1)$ 不属于 Z 中者, 易见 $\lambda_0 \geqslant 2$. 命

$$\delta = x_1 + y_1 + \lambda_0 (y_n - y_1) + y_1$$

显然有

$$\delta - y_1 \notin Z, \quad \delta - y_n \in Z.$$

今将 $y_1, \cdots, y_n$ 重新排列. 使

$$\begin{cases} \delta - y_s \notin Z, & 1 \leqslant s \leqslant r, \\ \delta - y_{s'} \in Z, & r < s' \leqslant n. \end{cases}$$

显然 $r \leqslant n-1$. 又命 Z' 表示由 $x_u + y_s (1 \leqslant u \leqslant m, 1 \leqslant s \leqslant r)$ 所成的集合, 则 Z' 为 Z 的一个部分集.

今往证明

$$\delta - y_{s'} \notin Z',$$

事实上, 若 $\delta - y_{s'} \in Z'$, 则由 $\delta - y_{s'} = x_u + y_s$ 推得

$$\delta - y_s = x_u + y_{s'} \in Z,$$

这与 $\delta - y_s \notin Z$ 相矛盾, 故 $\delta - y_{s'} \notin Z$. 命 t' 为由 Z' 所代表的不同的剩余系 $(\bmod p^l)$ 的个数, 则有

$$t' \leqslant t - (n-r).$$

又由归纳法假定

$$t' \geqslant m + r - 1$$

故得引理.

引理 8.8　当 $s \geqslant 3k$ 及 $(p-1) \nmid k$, 则

$$M_s(p^\gamma, N) > 0.$$

更确切些: 若 $k \neq \frac{1}{2}p^\theta(p-1)$, 则当 $s \geqslant 2k$ 时, 以上结论仍为正确. 当 $k = \frac{1}{2}p^\theta(p-1)$ 时, 则只当

$$N \equiv \pm s, \pm(s-2), \pm(s-4), \cdots, \quad (\bmod p^\gamma)$$

之一成立时, $M_s(p^\gamma, N) > 0$.

证　显然可知 $p > 2$.

1) $p \nmid k$, 则 $\gamma = 1$. 由 $(p-1) \nmid k$ 及引理 8.4, 可知 x^k 给与

$$d = \frac{p-1}{(k, p-1)} > 1$$

个不同的剩余系, mod$p$. 由引理 8.7, $x_1^k + \cdots + x_s^k (p \nmid x_1 \cdots x_s)$ 给与

$$\min(d + (d-1)(s-1), p)$$

个不同的剩余系, mod$p$. 当

$$s \geqslant 2k \geqslant \frac{p-1}{\frac{1}{2}d} \geqslant \frac{p-1}{d-1}$$

时,

$$\min(d + (d-1)(s-1), p) = p.$$

2) 设 $k = p^\theta k_0, p \nmid k_0$. 由于

$$x^{p^\theta k_0} \equiv x^{k_0} (\bmod p) \quad 及 (p-1) \nmid k_0,$$

所以 x^k 至少经过 $(p-1)/(p-1, k_0)(>1)$ 个不同的剩余系, mod$p$. 故

$$x_1^k + \cdots + x_s^k, \quad p \nmid x_1 \cdots x_s,$$

给与

$$\min\left(\frac{p-1}{(p-1, k_0)} + \left(\frac{p-1}{(p-1, k_0)} - 1\right)(s-1), p^\gamma\right)$$

个不同的剩余系, modp^γ.

当 $k_0 \nmid (p-1)$ 时, 因 $(p-1) \nmid k_0$, 易证

$$\frac{k_0(p-1)}{(k_0, p-1)} \geqslant k_0 + (p-1),$$

故

$$\frac{2k_0(p-1)}{(k_0,p-1)} \geqslant 2k_0+p.$$

又当 $p-1=mk_0$, 而 $m>2$ 时, 亦不难证明上式之真确. 由此推得当 $k \neq \frac{1}{2}p^{\theta}(p-1)$, 而 $s \geqslant 2k$ 时,

$$s-1 \geqslant 2p^{\theta}k_0-1 \geqslant \frac{p^{\gamma}}{\dfrac{p-1}{(p-1,k_0)}-1}-1,$$

因此 $x_1^k+\cdots+x_s^k(p \nmid x_1\cdots x_s)$ 给与 p^{γ} 个不同的剩余系.

又当 $k=\frac{1}{2}p^{\theta}(p-1)=\frac{1}{2}\varphi(p^{\gamma})$ 时, 则 $x^k \equiv \pm 1(\bmod p^{\gamma})$, 故只当 $N \equiv \pm s$, $\pm(s-2), \pm(s-4), \cdots, \pm(s-2\left[\frac{1}{2}s\right])(\bmod p^{\gamma})$ 时, $M_s(p^{\gamma},N)>0$. 但当 $s \geqslant 3k$ 时, 因 $s \geqslant p^{\gamma}$, 故不难证明 $\pm s, \pm(s-2), \pm(s-4), \cdots, \pm\left(s-2\left[\frac{1}{2}s\right]\right)$ 经过所有的剩余系, $\bmod p^{\gamma}$. 而引理得证.

引理 8.9　若 $s \equiv N(\bmod p^{\gamma})$, 则

$$M_s(p^{\gamma},N)>0.$$

此引理的证明十分明显.

§8.4　奇异级数的正性质

引理 8.10　当 $s>4$ 时, 奇异级数 $\mathfrak{S}(N)$ 绝对收敛. 当 $k=1$, 此结果可进一步改善为 $s>2$.

证　由引理 8.5 有

$$|\mathfrak{S}(N)| \leqslant \sum_{q=1}^{\infty}|B_s(N,q)| \ll \sum_{q=1}^{\infty} q^{1-\frac{1}{2}s+\varepsilon}.$$

当 $k=1$ 时, $W_{k,q}=\mu(q)$(Möbius 函数). 而 $|\mu(q)| \leqslant 1$, 故

$$|\mathfrak{S}(N)| \leqslant \sum_{q=1}^{\infty}|B_s(N,q)| \ll \sum_{q=1}^{\infty} q^{1-s+\varepsilon}.$$

引理 8.11　当 $s>4$ 时,

$$\mathfrak{S}(N)=\prod_{p} x_p(N),$$

此处

$$x_p(N) = 1 + \sum_{t=1}^{\gamma} B_s(N, p^t).$$

当 $k=1$, 此结果可以进一步改善为 $s>2$.

证　此引理可由引理 8.1, 8.3 及 8.10 直接推得.

引理 8.12　有一常数 A 存在, 使当 $s \geqslant 3k$ 时

$$\mathfrak{S}(N) \geqslant A > 0.$$

更清楚些: 若 $k \neq \frac{1}{2}p^{\theta}(p-1)$ 时, 则当 $s \geqslant 2k$ 时, 以上结论仍为真实. 若 $k = \frac{1}{2}p^{\theta}(p-1)$, 而

$$N \equiv \pm s, \pm(s-2), \pm(s-4), \cdots, \pm\left(s - 2\left[\frac{1}{2}s\right]\right) \pmod{p^{\gamma}}$$

时, 以上结果对于任何 s 仍为真确.

证　由引理 8.6, 8.8 及 8.9 已知: 对所有的 p,

$$x_p(N) > 0.$$

又

$$|B_s(N,p)| \leqslant p\left(\frac{3k\sqrt{p}}{p-1}\right)^s \leqslant (6k)^s p^{-\frac{1}{2}s+1}.$$

所以当 $p > (6k)^{4s}$ 时,

$$x_p > 1 - p^{-s/2+1+1/4}.$$

又当 $s>4$ 时,

$$\mathfrak{S}(N) \leqslant \prod_{p \leqslant (6k)^{4s}} x_p \prod_{p > (6k)^{4s}} (1 - p^{-5/4}) \geqslant A > 0.$$

同法证明 $k=1, s>2$ 的情况.

显然, 定理 12 可由引理 8.12 推得.

§8.5　定理 11 与 12 的推理

易于得出以下的定理: 假定 $s \geqslant s_0$, 而

$$s_0 \geqslant \begin{cases} 2^k + 1, & 若 1 \leqslant k \leqslant 10, \\ 2k^2(2\log k + \log\log k + 2.5), & 若 k > 10. \end{cases}$$

所有的充分大的 $\equiv s(\mathrm{mod} K)$ 的整数 N 可以表成 s 个素数的 k 次方的和.

为了更具体起见, 我们引出几个特例:

推理 1　所有的充分大的奇数是三素数的和.

推理 2　所有的充分大的 $\equiv 5(\mathrm{mod}\ 24)$ 的整数可以表成五个素数的平方之和.

推理 3　所有的充分大的奇数可以表成九个素数的立方的和.

推理 4　所有的充分大的 $\equiv 17(\mathrm{mod}\ 240)$ 的整数可以表成十七个素数的四次方之和.

今引入以下的定义以结束本章. 以 $H(k)$ 表有次之性质的最小整数 s: 所有的充分大的 $\equiv s(\mathrm{mod}\ K)$ 的整数可以表成 s 个素数的 k 乘方之和. 本章之结果可用下列的公式总结之:

$$H(k) \leqslant \begin{cases} 2^k + 1, & \text{若} 1 \leqslant k \leqslant 10, \\ 2k^2(2\log k + \log\log k + 2.5), & \text{若} k > 10. \end{cases}$$

第 9 章　华林–哥德巴赫问题进一步的研究

§9.1

本章的目的在于证明较第八章 §5 更好的结果. 今先引入指数密率的概念.

定义: 命 $\mathfrak{U}$ 为一自然数的集合, 其中元素各不相同. 用 u 表示 $\mathfrak{U}$ 中的元素, 而命

$$U(X)=\sum_{u\leqslant X}1$$

表 $\mathfrak{U}$ 中不大于 X 的元素的个数. 若 ν 为最大的实数使对任一 $\varepsilon>0$,

$$U(X)\gg X^{\upsilon-\varepsilon}$$

都成立者. 则称 ν 为集合 $\mathfrak{U}$ 的指数密率.

在本章的讨论中, 常假定 $k\geqslant 4$, 又命 $a=\dfrac{1}{k}$,

$$b=\begin{cases}2k^2(2\log k+\log\log k+3), & 当k>12,\\ 2^{k-1}, & 当k\leqslant 12\end{cases}$$

及

$$m=\left[\frac{\log\dfrac{1}{2}b+\log(1-2a)}{-\log(1-a)}\right].$$

本章的主要定理为

定理 13　命 N 为一充分大 (即 $\geqslant c(k)$) 的整数, $\mathfrak{U}$ 为一指数密率不小于 ν 的自然数集合, 而命

$$\delta=k-1+\max_{1\leqslant r\leqslant k-2}\min\left(2^{1-r},\frac{r+1-\nu(k-1)}{2^r-1+\nu}\right).$$

假定

$$1+\nu\delta>k\left(1-\frac{2}{b}\right),$$

且若

$$u+u'\equiv N-2k-3\pmod{K},\quad u,u'\in\mathfrak{U},\quad u,u'\leqslant X$$

的解的个数常 $\gg U^2(X)$, 则

i) 当 $k \neq \frac{1}{2}p^{\theta}(p-1)(p\neq 2)$ 时, N 能表成为

$$p_1^k + p_2^k + \cdots + p_{2k+3}^k + u + u', \quad u, u' \in \mathfrak{U} \tag{1}$$

的形式;

ii) 当 $k = \frac{1}{2}p^{\theta}(p-1)(p\neq 2)$ 时, 若对任何 $l, \mathfrak{U}$ 中适合

$$u \equiv l \pmod{p}$$

的元素所成集合 $\mathfrak{U}_l$ 的指数密率也不小于 ν, 则 N 也能表成 (1) 的形式.

引理 9.1　方程式

$$x_0^k + \cdots + x_{m-1}^k + x_m^k + x_m'^k = y_0^k + \cdots + y_{m-1}^k + y_m^k + y_m'^k \tag{2}$$

在区间

$$2^{-i}P^{(1-a)^i} \leqslant x_i, y_i \leqslant 2^{1-i}P^{(1-a)^i}, \quad 0 \leqslant i \leqslant m \tag{3}$$

内的整数解的组数为

$$O(P^{k-(k-2)(1-a)^m}L^{c_3}).$$

证　由 (2), (3) 二式可以得出: 当 P 充分大时, $x_i = y_i (i = 0, \cdots, m-1)$. 事实上, 假定 μ 是第一个使 $x_\mu \neq y_\mu$ 的足标, 则

$$\left|x_\mu^k - y_\mu^k\right| = k\left|\int_{y_\mu}^{x_\mu} t^{k-1}\mathrm{d}t\right| \geqslant k(2^{-\mu}P^{(1-a)\mu})^{k-1}$$

此不等式的右端当 P 相当大时大于

$$y_{\mu+1}^k + \cdots + y_m^k + y_m'^k,$$

因之, (2) 式变为不可能. 这证明了 $x_i = y_i (i = 0, \cdots, m-1)$. 又由定理 4, 方程

$$x_m^k + x_m'^k = y_m^k + y_m'^k,$$

的解数是 $O(P^{2(1-a)^m}L^{c_3})$. 引理于是得证.

引理 9.2　命 $q \geqslant 1$, 及 $l_0, \cdots, l_{m+1}$ 是一组整数, $(l_i, q) = 1$. 用 $\mathfrak{U}$ 表形如

$$u = p_0^k + \cdots + p_{m+1}^k, \quad p_i \equiv l_i \pmod{q} \tag{4}$$

的不同整数的集合, 此处 $p_i (0 \leqslant i \leqslant m+1)$ 经过算术级数 $qx + l_i$ 中的素数, 则 $\mathfrak{U}$ 的指数密率

$$\geqslant 1 - (1-2a)(1-a)^m.$$

证　命 $P=\left[\frac{1}{2}\left(\frac{X}{m+2}\right)^a\right]$, 易见 $P^k \ll X \ll P^k$.

$\mathfrak{U}$ 内不大于 X 的数中, 显然包有 u 之适合

$$\begin{aligned}&2^{-i}P^{(1-a)^i} \leqslant p_i \leqslant 2^{1-i}P(1-a)^i, \quad 0 \leqslant i \leqslant m,\\&2^{-m}P^{(1-a)^m} \leqslant p_{m+1} \leqslant 2^{1-m}P^{(1-a)^m}\end{aligned} \tag{5}$$

者. 命 $r(u)$ 表示方程式 (4) 在区间 (5) 内素数解组的个数. 则由 Gauchy 不等式得到

$$\left(\sum_u r(u)\right)^2 \leqslant U(X)\sum_u r^2(u).$$

由引理 9.1 易见

$$\sum_u r^2(u) \ll P^{k-(k-2)(1-a)^m+\varepsilon},$$

又由引理 7.14, 可知

$$\sum_u r(u) \gg P^{k-(k-2)(1-a)^m-\varepsilon},$$

故得

$$U(x) \gg P^{k-(k-2)(1-a)^m-\varepsilon} \gg X^{1-(1-2a)(1-a)^m-\varepsilon}.$$

此即引理.

在定理 13 中, 取 $\mathfrak{U}$ 为形如

$$u=p_0^k+\cdots+p_{m+1}^k$$

的不同整数的集合, 而取 $\nu=1-(1-2a)(1-a)^m$. 因 $\delta>k-1$, 故易见 $1+\nu\delta>k\left(1-\frac{2}{b}\right)$ 之成立. 又当 $k=\frac{1}{2}p^\theta(p-1)(p>2)$ 时, 必有 $k\geqslant 9$, 易证 $m+2\geqslant 3k$, 故由引理 8.8 同余式

$$l_0^k+\cdots+l_{m+1}^k \equiv l \pmod{p^\gamma}, \quad p\nmid l_0\cdots l_{m+1}$$

有解, 于是由引理 9.2 可知 $\mathfrak{U}_l$ 的指数密率也 $\geqslant \nu$. 因此得到

定理 14　命 $S_0=S_0(k)=2k+2m+7$ 及 $S\geqslant S_0$, 则所有的充分大的同余于 $S(\bmod K)$ 的整数 N, 是 S 个素数的 k 次方之和. 换言之

$$H(k)\leqslant 2k+2m+7.$$

当 k 充分大时,

$$m\sim 2k\log k$$

及

$$s_0 \sim 4k\log k.$$

此结果当 $k \geqslant 5$ 时较上章 §5 的结果为佳.

§9.2 Davenport 的引理

引理 9.3 (Davenport)*. 命 $\mathfrak{U}$ 表一由不相同的自然数所成的集合. $f(x)$ 表一 k 次整值多项式, δ 为一适合 $k-1<\delta\leqslant k$ 的实数, P 为一正整数, 则方程

$$f(x_1)+u_1=f(x_2)+u_2,\quad P\leqslant x_1,x_2\leqslant 2P,\ u_1,u_2\leqslant P^{\delta} \tag{1}$$

的解答的个数

$$\ll P^{1+\varepsilon}U(P^{\delta})(1+P^{\delta-k+1-2^{1-r}}+P^{(1-2^{-r})(\delta-k+1)-(r+1)2^{-r}}(U(P^{\delta}))^{2^{-r}}),$$

此处 r 适合于 $1\leqslant r\leqslant k-2$, 而符号 $\ll$ 所涉及的常数仅依于 k 及 ε.

证 引进符号

$$t_1\Delta f(x)=f(x+t_1)-f(x)$$

及

$$t_1\cdots t_r\Delta^r f(x)=t_r\Delta(t_1\cdots t_{r-1}\Delta^{r-1}f(x)).$$

1) 命 $N_r(r\geqslant 1)$ 代表下式的解数:

$$\begin{gathered}t_1\cdots t_r\Delta^r f(x)+u_1=u,\\ P\leqslant x\leqslant 2P,\ u_1,u\leqslant P^{\delta},\ t_1\cdots t_r\ll P^{\delta-k+r},\ t_i>0.\end{gathered} \tag{2}$$

对已定的 $t_1,\cdots,t_r$ 及 u, (2) 式的解数用 $r(u,t)$ 表它. 今往证明

$$N_r\ll U(P^{\delta})P^{\delta-k+r}+(U(P^{\delta})P^{\delta-k+r}N_{r+1})^{\frac{1}{2}}. \tag{3}$$

由 Cauchy 不等式可知

$$\begin{aligned}N_r&=\sum_t\sum_u r(u,t)\leqslant\left(\sum_t\sum_u 1\right)^{\frac{1}{2}}\left(\sum_t\sum_u r^2(u,t)\right)^{\frac{1}{2}}\\ &\ll\left(P^{\delta-k+r}U(P^{\delta})\sum_t\sum_u r^2(u,t)\right)^{\frac{1}{2}},\end{aligned}$$

*Rao 对这个引理提供了有价值的意见.

而 $\sum\limits_{t}\sum\limits_{u} r^2(u,t)$ 乃是下式的解数:

$$t_1\cdots t_r\Delta^r f(x_1)+u_1=t_1\cdots t_r\Delta^r f(x_2)+u_2, \tag{4}$$

并且此式的双方都限定在 $\mathfrak{U}$ 中. $t_1\cdots t_r\Delta^r f(x_2)+u_2$ 在 $\mathfrak{U}$ 中的个数显然就是 N_r. 因此当 $x_1=x_2$ 时, (4) 式的解数是 N_r. 今假定 $x_1>x_2$, 并命 $x_1=x+t_{r+1}$ 及 $x_2=x$ 则得

$$t_1\cdots t_{r+1}\Delta^{r+1} f(x)+u_1=u_2. \tag{5}$$

由于

$$\Delta^{r+1}f(x)\gg x^{k-r-1}\gg P^{k-r-1},$$

可知

$$t_1\cdots t_{r+1}\ll P^{\delta-k+r+1}.$$

故适合 $x_1>x_2$ 的 (4) 式的解数 $\ll N_{r+1}$. 因此得出

$$N_r\ll\{P^{\delta-k+r}U(P^\delta)(N_r+N_{r+1})\}^{\frac{1}{2}},$$

即

$$N_r\ll P^{\delta-k+r}U(P^\delta)+(P^{\delta-k+r}U(P^\delta)N_{r+1})^{\frac{1}{2}}.$$

2) 当 $1\leqslant r\leqslant k-2$ 时,

$$N_1\ll U(P^\delta)P^{\delta-k+2-2^{1-r}}+(U(P^\delta))^{1-2^{-r}}P^{(\delta-k+1)(1-2^{-r})+1-(r+1)^{2^{-r}}}N_{r+1}^{2^{-r}} \tag{6}$$

当 $r=1$ 时, (6) 式由 (3) 式得出. 现在假定 (6) 式对 $r-1$ 是真实的. 由 (3) 得出

$$\begin{aligned}N_r\ll&U(P^\delta)P^{\delta-k+2-2^{2-r}}+(U(P^\delta))^{1-2^{1-r}}P^{(\delta-k+1)(1-2^{1-r})+1-r2^{1-r}}N_r^{2^{1-r}}\\ \ll&U(P^\delta)P^{\delta-k+2-2^{2-r}}+(U(P^\delta))^{1-2^{1-r}}P^{(\delta-k+1)(1-2^{1-r})+1-r2^{1-r}}\\ &\times(U(P^\delta)P^{\delta-k+r}+(P^{\delta-k+r}U(P^\delta)N_{r+1})^{\frac{1}{2}})^{2^{1-r}}\\ \ll&U(P^\delta)P^{\delta-k+2-2^{1-r}}+(U(P^\delta))^{1-2^{-r}}P^{(\delta-k+1)(1-2^{-r})+1-(r+1)2^{-r}}N_{r+1}^{2^{-r}}.\end{aligned}$$

3) 命 N 表 (1) 式的解数, 今往证明

$$N\ll PU(P^\delta)+N_1.$$

若 $x_1=x_2$, 则 (1) 的解数 $\ll PU(P^\delta)$. 当 $x_1\neq x_2$, 则 (1) 的解数 $\ll N_1$.

由 (6) 式及显然的不等式

$$N_{r+1}\ll\sum_{u_1}\sum_{u_2}d^r(u_2-u_1)\ll(U(P^\delta))^2P^\varepsilon$$

而得出本引理.

§9.3　定理 13 的证明

命 $\mathfrak{U}$ 为一自然数集合, 其元素各不相同, 并假定其指数密率 $\geqslant v$. 又命

$$\delta = k-1+\max_{1\leqslant r\leqslant k-2}\min\left(2^{1-r}, \frac{r+1-v(k-1)}{2^r-1+v}\right),$$

显然当 $\nu > \frac{1}{k}$ 时, 可有 $\delta < k$.

命

$$\begin{aligned}
Q(\alpha) &= \sum_{\mu\leqslant P^\delta} \mathrm{e}^{2\pi \mathrm{i} w\alpha},\\
T(\alpha) &= \sum_{P\leqslant n\leqslant 2P} \mathrm{e}^{2\pi \mathrm{i} n^k\alpha},\\
\mathfrak{T}(\alpha) &= \sum_{P< p\leqslant 2P} \mathrm{e}^{2\pi \mathrm{i} p^k\alpha},\\
\mathfrak{T}^*(\alpha,h,q) &= \frac{W_{h,q}}{\varphi(q)}\sum_{P^k<n\leqslant(2P)^k}\frac{e(n\beta)}{n^{1-a}\log n}.
\end{aligned}$$

在引理 9.3 中, 取 $f(x)=x^k$, 则得

$$\int_0^1 |T(\alpha)Q(\alpha)|^2 \mathrm{d}\alpha \ll P^{1+\varepsilon}Q(0). \tag{1}$$

引理 9.4

$$\int_0^1 |T^{k+1}(\alpha)Q(\alpha)|^2 \mathrm{d}\alpha \ll P^{k+2}Q^2(0).$$

证　如第 7 章 §3 分割 $-\frac{1}{\tau}\leqslant\alpha\leqslant 1-\frac{1}{\tau}$.

1) 当 α 落入 E 内时, 由引理 3.6 及定理 9 已知

$$T(\alpha)\ll P^{1-\frac{1}{b}+\varepsilon},$$

故由 (1) 可得

$$\begin{aligned}
\int_E |T^{k+1}(\alpha)Q(\alpha)|^2 \mathrm{d}\alpha &\ll P^{2k(1-\frac{1}{b})+\varepsilon}\int_0^1 |T(\alpha)Q(\alpha)|^2\mathrm{d}\alpha\\
&\ll P^{2k(1-\frac{1}{b})+\varepsilon}P^{1+\varepsilon}Q(0)\ll P^{k+2}Q^2(0).
\end{aligned}$$

(此处用到 $1+v\delta > k\left(1-\frac{2}{b}\right)$ 的假定).

2) 由引理 7.12 可得

$$\sum_{\mathfrak{M}} \int_{\mathfrak{M}} |T^{k+1}(\alpha)Q(\alpha)|^2 \mathrm{d}\alpha \ll Q^2(0) \sum_{\mathfrak{M}} \int_{\mathfrak{M}} |T^{k+1}(\alpha)|^2 \mathrm{d}\alpha$$
$$\ll P^{k+2}Q^2(0).$$

由此得出本引理.

引理 9.5

$$\int_0^1 \mathfrak{T}^{2k+3}(\alpha)Q^2(\alpha)e(-N\alpha)\mathrm{d}\alpha$$
$$=\Psi(N) \sum_{u \leqslant P^\delta} \sum_{u' \leqslant P^\delta} \mathfrak{S}(N-u-u') + O(Q^2(0)P^{k+3}L^{-\eta}).$$

此处 η 系一大于 $2k+4$ 的常数. $\mathfrak{S}(N)$ 为当 $S=2k+3$ 时的奇异级数, 而

$$\Psi(N) = \sum_{\substack{n_1+\cdots+n_{2k+3}=N \\ P^k \leqslant n_i \leqslant (2P)^k}} \frac{1}{\prod_{i=1}^{2k+3} n_i^{1-a} \log n_i}.$$

证 如第七章 §7 分割 $-\frac{1}{\tau} \leqslant \alpha \leqslant 1-\frac{1}{\tau}$, 但此处我们选择了 σ 使定理 10 中的 σ_0 大于 η.

1) 由定理 10 可得

$$\int_E |\mathfrak{T}^{2k+3}(\alpha)Q^2(\alpha)|\mathrm{d}\alpha \ll \max_{\alpha \in E} |\mathfrak{T}(\alpha)| \int_0^1 |T^{k+1}(\alpha)Q(\alpha)|^2 \mathrm{d}\alpha$$
$$\ll Q^2(0)P^{k+3}L^{-\eta}.$$

2) 当 $\alpha \in \mathfrak{M}(h,q)$ 时,

$$\left|Q(\alpha) - Q\left(\frac{h}{q}\right)\right| \ll \sum_{u \leqslant P^\delta} \left|e\left(u\left(\frac{h}{q}+\beta\right)\right) - e\left(u\frac{h}{q}\right)\right|$$
$$\ll \sum_{u \leqslant P^\delta} |\beta| u \ll Q(0)P^\delta (qNL^{-\sigma})^{-1} \ll P^{\delta-k+\varepsilon}Q(0)$$

立得

$$\left|Q^2(\alpha) - Q^2\left(\frac{h}{q}\right)\right| \ll P^{\delta-k+\varepsilon}Q^2(0).$$

故由引理 7.16 可知

$$\sum_{\mathfrak{M}} \int_{\mathfrak{M}} |\mathfrak{Y}^{2k+3}(\alpha)| \left|Q^2(\alpha) - Q^2\left(\frac{h}{q}\right)\right| \mathrm{d}\alpha$$

$$\ll P^{\delta-k+\varepsilon}Q^2(0)\sum_{q\leqslant L^\sigma} q\cdot q^{-(2+3a)+\varepsilon}\left(\int_0^{P^{-k}} P^{2k+3}\mathrm{d}\beta+\int_{P^{-k}}\beta^{-2-3a}\mathrm{d}\beta\right)$$

$$\ll Q^2(0)P^{\delta+3+\varepsilon}\ll Q^2(0)P^{k+3}L^{-\eta}.$$

3) 如定理 11′ 证明中之 3) 可知

$$\sum_{\mathfrak{M}} Q^2\left(\frac{h}{q}\right)\int_{\mathfrak{M}}(\mathfrak{T}^{2k+3}(\alpha)-\mathfrak{T}^{*2k+3}(\alpha,h,q))e(-\alpha N)\mathrm{d}\alpha$$

$$\ll Q^2(0)\sum_{q\leqslant L^\sigma} q\cdot q^{-(2+2a)+\varepsilon}P^{k+3}\mathrm{e}^{-c\sqrt{L}}$$

$$\ll Q^2(0)P^{k+3}L^{-\eta}.$$

4) 如定理 11′ 证明中之 4) 可知

$$\sum_{\mathfrak{M}} Q^2\left(\frac{h}{q}\right)\left(\int_{-\frac{1}{2}}^{\frac{1}{2}}-\int_{\mathfrak{M}}\right)\mathfrak{T}^{*2k+3}(\alpha,h,q)e(-N\alpha)\mathrm{d}\beta$$

$$\ll Q^2(0)\sum_{q\leqslant L^\sigma} q\cdot q^{-(2+3a)+\varepsilon}\int_{q^{-1}N^{-1}L^\sigma}\beta^{-(2+3a)}\mathrm{d}\beta\ll Q^2(0)P^{k+3}L^{-\eta}.$$

(证明中用到 $3a\sigma>\sigma_0>\eta$).

5) 因为

$$\int_{-\frac{1}{2}}^{\frac{1}{2}}\mathfrak{T}^{*2k+3}(\alpha,h,q)e(-N\beta)\mathrm{d}\beta=\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2k+3}\Psi(N),$$

而由引理 7.19 可得

$$\Psi(N)\left(\sum_{u\leqslant P^\delta}\sum_{u'\leqslant P^\delta}\mathfrak{S}(N-u-u')-\sum_{\mathfrak{M}} Q^2\left(\frac{h}{q}\right)e\left(-N\frac{h}{q}\right)\left(\frac{W_{h,q}}{\varphi(q)}\right)^{2k+3}\right)$$

$$\ll Q^2(0)P^{k+3}L^{-\eta}.$$

由以上的讨论, 可得引理.

由引理 7.19 易见

$$P^{k+3}L^{-2k-3}\ll\Psi(N)\ll P^{k+3}L^{-2k-3}.$$

因此由引理 9.5 及引理 8.12, 定理 13 得到证明.

§9.4 附　　记

命 $f(x)$ 为一首项系数为正的 k 次整值多项式.

引理 9.6 　命 $\mathfrak{U}$ 表一指数密率 $\geqslant \nu$ 的集合, 而命 $\mathfrak{B}$ 表形如

$$\nu = f(p) + u$$

的不同整数的集合. 则 $\mathfrak{B}$ 的指数密率不小于 $a(1+\delta\nu)$. δ' 的定义见 §1 定理 13.

证 　命 x_0 为方程式 $X = f(x)$ 的最大正根. 而命 $P = \left[\frac{1}{4}x_0\right]$. 显然有 $P^k \ll X \ll P^k$.

当 X 充分大时 $\mathfrak{B}$ 内不大于 X 的数中显然包有

$$f(p) + u, \quad P \leqslant p \leqslant 2P, \quad u \leqslant P^\delta.$$

命 $r(\nu)$ 表示方程

$$\nu = f(p) + u, \quad P \leqslant x \leqslant 2P, \quad u \leqslant P^\delta$$

的解数. 则由 Cauchy 不等式得到

$$\left(\sum_\nu r(v)\right)^2 \leqslant \left(\sum_\nu 1\right)\left(\sum_\nu r^2(v)\right).$$

因 $\sum\limits_v r^2(\nu)$ 不大于

$$f(x_1) + u_1 = f(x_2) + u_2, \quad P \leqslant x_1, x_2 \leqslant 2P, \quad u_1, u_2 \leqslant P^\delta$$

的解数, 故由引理 9.3 得到

$$\sum_\nu r^2(\nu) \ll P^{1+\varepsilon} U(P^\delta).$$

又因

$$\sum_\nu r(\nu) \gg P^{1-\varepsilon} U(P^\delta) \quad 及 U(P^\delta) \gg P^{\nu\delta-\varepsilon},$$

故得

$$V(X) \gg \sum_\nu 1 \gg P^{1+\nu\delta-\varepsilon} \gg X^{a(1+\nu\delta)-\varepsilon},$$

而得引理.

引理 9.7　命 $f(x)$ 表一首项系数为正的四次整值多项式. 而命 $\mathfrak{B}_4$ 表形如

$$\nu = f(p_1) + f(p_2) + f(p_3) + f(p_4)$$

的不同整数的集合. 则 $\mathfrak{B}_4$ 的指数密率 $\geqslant \frac{331}{412}$.

证　1) 命 $\mathfrak{U}$ 为形如

$$u = f(p_1) + f(p_2)$$

的不同整数的集合. 在 $\mathfrak{U}$ 中不大于 X 的数中显然包有

$$u = f(p_1) + f(p_2), \quad P \leqslant p_1, p_2 \leqslant 2P.$$

此处 $P = \left[\frac{1}{4}x_0\right]$. 而 x_0 为 $X = f(x)$ 的最大正根. 又命 $r(u)$ 表上式的解数. 则因

$$\sum_u r(u) \gg P^{2-\varepsilon} \gg X^{\frac{1}{2}-\varepsilon},$$

并由定理 4 得到

$$\sum_u r^2(u) \leqslant \int_0^1 \left|\sum_{x=1}^{2P} e(\alpha f(x))\right|^4 \mathrm{d}\alpha \ll P^{2+\varepsilon} \ll X^{\frac{1}{2}+\varepsilon},$$

及 Cauchy 公式

$$\left(\sum_u r(u)\right)^2 \leqslant \left(\sum_u 1\right)\left(\sum_u r^2(u)\right)$$

因而得到

$$U(X) \gg \sum_u 1 \gg X^{\frac{1}{2}-\varepsilon}.$$

2) 在引理 9.6 中. 取 $\nu = \frac{1}{2}, r = 2, \delta = \frac{24}{7}$, 则由形如

$$f(p_1) + f(p_2) + f(p_3)$$

的不同整数所成的集合的指数密率 $\geqslant \frac{1}{4}\left(1 + \frac{1}{2}\cdot\frac{24}{7}\right) = \frac{19}{28}$.

再用引理 9.6, 但取 $\nu = \frac{19}{28}, r = 2, \delta = \frac{336}{103}$, 而得出 $\mathfrak{B}_4$ 的指数密率

$$\geqslant \frac{1}{4}\left(1 + \frac{19}{28}\cdot\frac{336}{103}\right) = \frac{331}{412}.$$

为了清楚起见, 我们把这证明列为下表: 表中 n 为 $f(x)$ 的个数, ν_n 表示由形如

$$f(p_1) + f(p_2) + \cdots + f(p_n)$$

的不同整数所成集合的指数密率.

n	r	δ	$\nu_n \geqslant$
2	–	–	$\frac{1}{2}$
3	2	$\frac{24}{7}$	$\frac{19}{28}$
4	2	$\frac{336}{103}$	$\frac{331}{412}$

引理 9.8　命 $f(x)$ 表一五次的整值多项式. 而命 $\mathfrak{B}_7$ 表形如

$$f(p_1)+f(p_2)+\cdots+f(p_7)$$

的不同整数的集合. 则 $\mathfrak{B}_7$ 的指数密率

$$\geqslant \frac{1}{5}\cdot\frac{127,6889}{29,1873}.$$

这引理的证明可用下表说明它：

n	r	δ	$\nu_n \geqslant$
2	–	–	$\frac{2}{5}$
3	2	$5\cdot\frac{15}{17}$	$\frac{1}{5}\cdot\frac{47}{17}$
7	3	–	$\frac{1}{5}\cdot\frac{127,6889}{29,1873}$

说明　$\nu_4,\cdots,\nu_7$ 可由 $\nu_3\geqslant\frac{1}{5}\cdot\frac{47}{17}$ 连续运用公式

$$\nu_{n+1}\geqslant\frac{1}{5}\left(1+\frac{32\nu_n}{7+\nu_n}\right),\quad n\geqslant 3$$

而得出. 在计算时运用此式可以更为便捷：

$$\frac{5\nu_{n+1}+7}{1-\nu_{n+1}}\geqslant\frac{10}{7}\frac{5\nu_n+7}{1-\nu_n},\quad n\geqslant 3.$$

引理 9.9　命 $f(x)$ 代表一个六次整值多项式. 而命 $\mathfrak{B}_{12}$ 表形如

$$f(p_1)+f(p_2)+\cdots+f(p_{12})$$

的不同整数的集合. 则 $\mathfrak{B}_{12}$ 的指数密率 $\geqslant 0.934$.

此引理可由下表以说明之：

n	r	δ	$\nu_n \geqslant$
2	–	–	$\frac{1}{3}$
3	2	$6\cdot\frac{9}{10}$	$\frac{1}{6}\cdot\frac{14}{5}$
4	3	$6\cdot\frac{195}{224}$	$\frac{1}{6}\cdot\frac{55}{16}$
5	3	$6\cdot\frac{624}{727}$	$\frac{1}{6}\cdot\frac{2872}{727}$
12	4	–	0.934

说明　数值 0.934 是由 $\nu_5 \geqslant \frac{1}{6}\cdot\frac{2872}{727}$ 经公式

$$\nu_{n+1} \geqslant \frac{1}{6}\left(1+\frac{80\nu_n}{15+\nu_n}\right), \quad 即\frac{2\nu_{n+1}+5}{1-\nu_{n+1}} \geqslant \frac{32}{25}\frac{2\nu_n+5}{1-\nu_n}, \quad n \geqslant 5$$

连续运用而得出.

引理 9.10　命 $f(x)$ 代表一个七次整值多项式. 而命 $\mathfrak{B}_{18}$ 表形如

$$f(p_1)+f(p_2)+\cdots+f(p_{18})$$

的不同整数的集合. 则 $\mathfrak{B}_{18}$ 的指数密率

$$\geqslant 0.9601.$$

此引理可由下表以证明之.

n	r	δ	$\nu_n \geqslant$
2	–	–	$\frac{2}{7}$
3	2	$7\cdot\frac{21}{23}$	$\frac{1}{7}\cdot\frac{65}{23}$
4	3	$7\cdot\frac{529}{596}$	$\frac{1}{7}\cdot\frac{2091}{596}$
5	3	$7\cdot\frac{2,7416}{3,1295}$	$\frac{1}{7}\cdot\frac{12,7481}{3,1295}$
6	4	$7\cdot\frac{297,3025}{341,3456}$	$\frac{1}{7}\cdot\frac{1552,4151}{341,3456}$
7	4	$7\cdot\frac{3,2427,8320}{3,7393,7031}$	$\frac{1}{7}\cdot\frac{18,4873,1376}{3,7393,7031}$
18	5	–	0.9601

说明　数值 0.9601 是由 $\nu_7 \geqslant \frac{1}{7}\cdot\frac{18,4873,1376}{3,7393,7031}$ 连续运用公式

$$\nu_{n+1} \geqslant \frac{1}{7}\left(1+\frac{192\nu_n}{31+\nu_n}\right),\quad 即\frac{31+7\nu_{n+1}}{1-\nu_{n+1}} \geqslant \frac{112}{93}\frac{31+7\nu_n}{1-\nu_n},\quad n \geqslant 7$$

而得出

引理 9.11　命 $f(x)$ 代表一个八次整值多项式. 而命 $\mathfrak{B}_{28}$ 表形如

$$f(p_1)+f(p_2)+\cdots+f(p_{28})$$

的不同整数的集合. 则 $\mathfrak{B}_{28}$ 的指数密率

$$\geqslant 0.9838.$$

此引理可由下表以说明之:

n	r	δ	$v_n \geqslant$
2	—	—	$\frac{1}{4}$
3	2	$8\cdot\frac{12}{13}$	$\frac{1}{8}\cdot\frac{37}{13}$
4	3	$8\cdot\frac{689}{765}$	$\frac{1}{8}\cdot\frac{2726}{765}$
5	4	$8\cdot\frac{4,2075}{4,7263}$	$\frac{1}{8}\cdot\frac{19,7193}{4,7263}$
6	4	$8\cdot\frac{519,8930}{586,8753}$	$\frac{1}{8}\cdot\frac{2755,9983}{586,8753}$
7	5	$8\cdot\frac{13,0873,1919}{14,8301,0727}$	$\frac{1}{8}\cdot\frac{76,2888,6936}{14,8301,0727}$
8	5	$8\cdot\frac{3307,1139,2121}{3754,1554,7232}$	$\frac{1}{8}\cdot\frac{2595,8216,6745}{469,2694,3404}$
9	5	$8\cdot\frac{10,4647,0837,9092}{11,8974,6413,0937}$	$\frac{1}{8}\cdot\frac{69,7842,8731,5072}{11,8974,6413,0937}$
28	6	—	0.9838

说明　数值 0.9838 是由 $\nu_9 \geqslant \frac{1}{8}\cdot\frac{69,7842,8731,5072}{11,8974,6413,0937}$ 连续运用公式

$$\nu_{n+1} \geqslant \frac{1}{8}\left(1+\frac{448\nu_n}{63+\nu_n}\right),\quad 即\frac{8\nu_{n+1}+63}{1-\nu_{n+1}} \geqslant \frac{512}{441}\frac{8\nu_n+63}{1-\nu_n},\quad n \geqslant 9$$

而得到.

利用这些引理可以改进当 k 较小时 $H(k)$ 的上限. 例如: $H(4) \leqslant 15, H(5) \leqslant 25$ 等等. 但我们必须注意, 引理 9.4 中 $T(\alpha)$ 的次数不能再取为 $2(k+1)$. 为了达到上述目的, 在方法上我们还必须作适当的修改和改进.

第 10 章　素数未知数的不定方程组 *

§10.1

在本章及下一章中将讨论不定方程组：

$$p_1^k + \cdots + p_s^k = N_k,$$
$$\cdots\cdots$$
$$p_1 + \cdots + p_s = N_1,$$

其中未知数 $p_1, \cdots, p_s$ 是素数. 本章中将给与此方程组的解数的渐近式, 而假定了 $s \geqslant s_0$, 此 s_0 的数值如下表:

k	2	3	4	5	6	7	8	9	10	$\geqslant 11$
s_0	7	19	49	113	243	417	675	1083	1773	$2k^2(3\log k + \log\log k + 4) - 21$

为了免除琐碎的枝节运算, 我们的证明中将假定 $k \geqslant 3$. 关于 $k = 2$ 的情况, 读者可以依据这一证明, 做适当的而不困难的修整, 得出证明.

§10.2　证明定理 16 所需要的几条引理

引理 10.1**　命 $\gamma_k, \cdots, \gamma_1$ 表 k 个实数. 且命

$$I = \int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x)\mathrm{d}x,$$

则

$$I \ll Z, \quad Z = (\max(1, |\gamma_1|, \cdots, |\gamma_k|))^{-a}.$$

证　显然 $|I| \leqslant 1$. 故可假定 $|\gamma_h| \geqslant 1, (1 \leqslant h \leqslant k)$. 我们有

$$I^k = \int_0^1 \cdots \int_0^1 e(\psi)\mathrm{d}x_1 \cdots \mathrm{d}x_k,$$

---

* 关于第十章及第十一章中所讨论的问题可比较 К. К. Марджанищвили “Об олной залаче аддитивной теории чисел”. Изв, АН СССР, Серин математическая, Т. 4(1940), стр. 193-194, (俄文本译者注).

** И. М. Виноградов, Матемамический сборник, 3(1938), 435-471; 这一证明见华罗庚, 等幂和问题解数的研究, 数学学报, 2(1952).

此处

$$\psi = (x_1^k + \cdots + x_k^k)\gamma_k + \cdots + (x_1 + \cdots + x_k)\gamma_1.$$

显然有

$$I^k = k! \int\limits_{0\leqslant x_1\leqslant x_2\leqslant\cdots\leqslant x_k\leqslant 1}\cdots\int e(\psi)\mathrm{d}x_1\cdots\mathrm{d}x_k.$$

今讨论变换

$$\left.\begin{aligned}(x_1^k+\cdots+x_k^k)|\gamma_k| &= y_k,\\ &\cdots\cdots\\ (x_1+\cdots+x_k)|\gamma_1| &= y_1.\end{aligned}\right\}$$

以 $\mathfrak{R}$ 代表当 $x_1,\cdots,x_k$ 属于域 $0\leqslant x_1\leqslant x_2\leqslant\cdots\leqslant x_k\leqslant 1$ 时 $y_1,\cdots,y_k$ 所绘出的域. 此变换的函数行列式

$$\frac{\partial(x_1,\cdots,x_k)}{\partial(y_1,\cdots,y_k)} = g(y_1,\cdots,y_k)$$

经常是正号. 引用引理 7.5 可得

$$\begin{aligned}|k!^{-1}I^k| &= \left|\int\underset{\mathfrak{R}}{\cdots}\int e(\pm y_k\pm\cdots\pm y_1)g(y_1,\cdots,y_k)\mathrm{d}y_1\cdots\mathrm{d}y_k\right|\\
&\leqslant \int\cdots\int \mathrm{d}y_1\cdots\mathrm{d}y_{h-1}\mathrm{d}y_{h+1}\cdots\mathrm{d}y_k\left|\int e(\pm y_h)g(y_1,\cdots,y_k)\mathrm{d}y_h\right|\\
&\ll \max_{0\leqslant\xi\leqslant 1}\int\cdots\int \mathrm{d}y_1\cdots\mathrm{d}y_{h-1}\mathrm{d}y_{h+1}\cdots\mathrm{d}y_k\max_v\int\limits_{v\leqslant y_h\leqslant v+\xi} g(y_1,\cdots,y_k)\mathrm{d}y_k\\
&\ll \max_{\substack{0\leqslant\xi\leqslant 1\\ v}}\underset{v\leqslant y_h\leqslant v+\xi}{\int_0^1\cdots\int_0^1}\mathrm{d}x_1\cdots\mathrm{d}x_k.\end{aligned}\tag{1}$$

今有

$$\begin{aligned}\underset{v\leqslant y_h\leqslant v+\xi}{\int_0^1\cdots\int_0^1}\mathrm{d}x_1\cdots\mathrm{d}x_k &\leqslant \underset{v\leqslant y_h\leqslant v+\xi}{\int\cdots\int}\mathrm{d}x_1\cdots\mathrm{d}x_k \leqslant \underset{v\leqslant y_h\leqslant v+1}{\int\cdots\int}\mathrm{d}x_1\cdots\mathrm{d}x_k\\
&= V(v+1)-V(v),\end{aligned}\tag{2}$$

此处 $V(v)$ 是由

$$y_h = |\gamma_h|(x_1^h+\cdots+x_k^h)\leqslant v,\quad x_v\geqslant 0,$$

所定义的域的体积. 因

$$V(v) = \eta\left(\frac{v}{|\gamma_h|}\right)^{k/h}$$

(此处 η 是一个依于 h 及 k 的常数), 所以

$$\begin{aligned}V(v+1)-V(v) &\ll \left(\frac{v+1}{|\gamma_h|}\right)^{k/h}-\left(\frac{v}{|\gamma_h|}\right)^{k/h}\\ &\ll |\gamma_h|^{-k/h}\int_v^{v+1} t^{k/h-1}\mathrm{d}t\\ &\ll |\gamma_h|^{-k/h}(v+1)^{k/h-1}\\ &\ll |\gamma_h|^{-k/h}(|\gamma_h|k+1)^{k/h-1}\end{aligned} \tag{3}$$

(其中用 $v\leqslant k|\gamma_h|$). 综合 (1), (2) 及 (3), 可得

$$\begin{aligned}I^k &\ll |\gamma_h|^{-k/h}(|\gamma_h|k+1)^{k/h-1}\\ &\ll |\gamma_h|^{-k/h-1+k/h}=|\gamma_h|^{-1}.\end{aligned}$$

这证明了本引理.

引理 10.2　仍如引理 10.1 的假定, 命 $\delta_v=\max(1,|\gamma_v|)$, 则

$$I\ll\prod_{v=1}^{k}\delta_v^{-a^2}.$$

又当 $0<\delta\leqslant 1$ 时,

$$\int_0^{\delta} e(\gamma_k x^k+\cdots+\gamma_1 x)\mathrm{d}x\ll\prod_{v=1}^{k}\delta_v^{-a^2}.$$

又当 $g>k^2$ 时,

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|I|^g\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1$$

收敛.

证　由于

$$\prod_{v=1}^{k}\delta_v=\prod_{v=1}^{k}\max(1,|\gamma_v|)\leqslant\max(1,|\gamma_1|,\cdots,|\gamma_k|)^k,$$

故由引理 10.1 立刻得出第一个不等式.

再,

$$\begin{aligned}\int_0^{\delta} e(\gamma_k x^k+\cdots+\gamma_1 x)\mathrm{d}x &= \delta\int_0^1 e(\gamma_k\delta^k y^k+\cdots+\gamma_1\delta y)\mathrm{d}y\\ &\ll \delta\left(\prod_{v=1}^{k}\max(1,\delta^v|\gamma_v|)\right)^{-a^2}\end{aligned}$$

$$\ll \delta\left(\prod_{v=1}^{k}\max(\delta^v,\delta^v|\gamma_v|)\right)^{-a^2}$$

$$\ll \delta^{\frac{1}{2}-\frac{1}{2}a}\left(\prod_{v=1}^{k}\delta_v\right)^{-a^2}\ll\left(\prod_{v=1}^{k}\delta_v\right)^{-a^2}.$$

这就证明了第二个不等式.

又积分

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|I|^g\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1\ll\prod_{v=1}^{k}\int_{-\infty}^{\infty}\delta_v^{-a^2g}\mathrm{d}\gamma_v$$

当 $g>k^2$ 时显然收敛.

引理 10.3 命 $q_1,\cdots,q_k$ 是正整数, $H=q_1\cdots q_k$, 又命 Q 代表 $q_1,\cdots,q_k$ 的最小公倍数,

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\frac{1}{H}\sum_{y=1}^{H}e\left(\frac{h_k}{q_k}y^k+\cdots+\frac{h_1}{q_1}y\right),\quad (h_v,q_v)=1,$$

则

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\ll Q^{-a+g}$$

且级数

$$\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}\sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1}\cdots\sum_{\substack{h_k=1\\(h_k,q_k)=1}}^{q_k}\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^g$$

当 $g>k(k+1)$ 时收敛.

证 先证明

$$\left(\frac{h_k}{q_k}Q,\cdots,\frac{h_1}{q_1}Q,Q\right)=1.$$

若不然, 必有一素数 p 使

$$p\,\Big|\left(\frac{h_k}{q_k}Q,\cdots,\frac{h_1}{q_1}Q,Q\right).$$

假定 p^b 能整除 Q, 而 p^{b+1} 不能整除 Q. 由 Q 的定义, 必有一 q, 命之为 q_l, 能为 p^b 所整除, 但不能为 p^{b+1} 所整除, 即 $\dfrac{h_l}{q_l}Q$ 不是 p 的倍数. 这和以上的假定相连.

由定理 1 可知

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\frac{1}{Q}\sum_{x=1}^{Q}e(g(x)/Q)\ll Q^{-a+\varepsilon},$$

此处

$$g(x)=Q\frac{h_k}{q_k}x^k+\cdots+Q\frac{h_1}{q_1}x.$$

由此推得, 引理中所讨论的无穷级数

$$\ll\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}\sum_{h_1=1}^{q_1}\cdots\sum_{h_k=1}^{q_k}Q^{-ag+\varepsilon}\leqslant\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}q_1\cdots q_kQ^{-ag+\varepsilon}.$$

对一固定的 Q, 我们来讨论和

$$\sigma(Q)=\sum\cdots\sum q_1\cdots q_k,$$

此和经过所有可能的最小公倍数为 Q 的整数组 $q_1,\cdots,q_k$. 由引理 2.1 可知

$$\sigma(Q)\leqslant\left(\sum_{q|Q}q\right)^k\ll Q^k(d(Q))^k\ll Q^{k+\varepsilon}.$$

所以该级数

$$\ll\sum_{Q=1}^{\infty}Q^{k-ag+\varepsilon}.$$

显然当 $k-ag<-1$ 时, 此级数收敛, 即 $g>k(k+1)$ 时, 原级数收敛.

附记: 引理 10.2 及 10.3 的收敛指数都还可改善. 请参考数学学报第二卷华罗庚著文.

引理 10.4　命

$$f(x)=\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x,(h_v,q_v)=1,q_v\geqslant 1.$$

又命 Q_1 是 $q_k,\cdots,q_2$ 的最小公倍数, Q 是 Q_1 及 q_1 的最小公倍数. 假定 $Q_1<Q$, 则

$$\sum_{x=1}^{p}e(f(x))\ll Q.$$

证　当 $Q\geqslant P$ 时, 这引理显然正确. 假定 $Q<P$. 命 $x=Q_1y+z$, 此处

$$1\leqslant z\leqslant Q_1,\quad 0\leqslant y\leqslant(P-z)/Q_1.$$

因为 q_1 不能整除 Q_1, 所以

$$\left|\sum_{x=1}^{P}e(f(x))\right|=\left|\sum_{z=1}^{Q_1}e(f(z))\sum_{y=0}^{(P-z)/Q_1}\mathrm{e}^{2\pi\mathrm{i}h_1Q_1y/q_1}\right|$$

$$\leqslant Q_1 \max_z \left| \sum_y \mathrm{e}^{2\pi \mathrm{i} h_1 Q_1 y/q_1} \right|$$

$$\leqslant \frac{Q_1}{(h_1 Q_1/q_1)} \leqslant \frac{Q_1 q_1}{(Q_1, q_1)} = Q$$

(用了引理 1.8).

引理 10.5 命 σ 是一小于 $\frac{1}{4}a$ 的正数, 及

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x.$$

又命

$$\alpha_v = \frac{h_v}{q_v} + \frac{\theta_v}{q_v \tau_v}, \quad |\theta_v| \leqslant 1, \quad (h_v, q_v) = 1,$$

其中

$$\tau_1 = P^{\frac{1}{2}}, \quad \tau_v = P^{v - \frac{1}{2}a + \sigma}, \quad 2 \leqslant v \leqslant k.$$

假定

$$P^{\frac{1}{2} - \frac{1}{2}a + \sigma} < q_1 \leqslant \tau_1, \quad q_v \leqslant P^{\frac{1}{2}a - 2\sigma}, \quad 2 \leqslant v \leqslant k,$$

则

$$\sum_{x=1}^{P} e(f(x)) \ll P^{1-\sigma}.$$

证 命

$$S_n = \sum_{x \leqslant n} e\left(\frac{h_k}{q_k} x^k + \cdots + \frac{h_1}{q_1} x \right).$$

由于 $Q_1 \leqslant q_2 \cdots q_k < P^{(k-1)(\frac{1}{2}a - 2\sigma)} = P^{\frac{1}{2} - \frac{1}{2}a - 2\sigma(k-1)} < P^{\frac{1}{2} - \frac{1}{2}a + \sigma} < q_1$, 根据引理 10.4, 可知

$$S_n \ll Q \leqslant q_2 \cdots q_k$$
$$\leqslant P^{\frac{1}{2}} \cdot P^{(\frac{1}{2}a - 2\sigma)(k-1)} \ll P^{1 - \frac{1}{2}a - 2\sigma(k-1)}.$$

又如命 $\theta_v / q_v \tau_v = \beta_v, (1 \leqslant v \leqslant k)$, 则

$$\sum_{x=1}^{P} e(f(x)) = \sum_{n=1}^{P} (S_n - S_{n-1}) e(\beta_k n^k + \cdots + \beta_1 n)$$
$$= \sum_{n=1}^{P} S_n (e(\beta_k n^k + \cdots + \beta_1 n) - e(\beta_k (n+1)^k + \cdots + \beta_1 (n+1)))$$
$$+ S_P e(\beta_k (P+1)^k + \cdots + \beta_1 (P+1)).$$

因为

$$\begin{aligned}
&|e(\beta_k(n+1)^k+\cdots+\beta_1(n+1))-e(\beta_k n^k+\cdots+\beta_1 n)|\\
&\ll |\beta_k|P^{k-1}+|\beta_{k-1}|P^{k-2}+\cdots+|\beta_1|\\
&\ll \frac{P^{k-1}}{\tau_k}+\frac{P^{k-2}}{\tau_{k-1}}+\cdots+\frac{P}{\tau_2}+\frac{1}{q_1\tau_1}\\
&\ll P^{-1+\frac{1}{2}a-\sigma}+P^{-\frac{1}{2}-\frac{1}{2}+\frac{1}{2}a-\sigma}\ll P^{-1+\frac{1}{2}a-\sigma},
\end{aligned}$$

所以

$$\begin{aligned}
\sum_{x=1}^{P}e(f(x))&\ll\sum P^{1-\frac{1}{2}a-2\sigma(k-1)}P^{-1+\frac{1}{2}a-\sigma}\\
&\ll P^{1-\sigma(2k-1)}\ll P^{1-\sigma}.
\end{aligned}$$

§10.3　关于 Tarry 问题的结果

定理 15　命

$$S(\alpha_k,\cdots,\alpha_1)=\sum_{x\leqslant P}e(\alpha_k x^k+\cdots+\alpha_1 x).$$

命 t_0 表一与 k 有关的正整数, 它的定义如下表:

k	2	3	4	5	6	7	8	9	10	$\geqslant 11$
t_0	3	8	23	55	120	207	336	540	885	$[k^2(3\log k+\log\log k+4)]-11$

则当 $t>t_0$ 时, 有下面的结果

$$\begin{aligned}
T(P)&=\int_0^1\cdots\int_0^1|S(\alpha_k,\cdots,\alpha_1)|^{2t}\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1\\
&=c_1c_2P^{2t-\frac{1}{2}k(k+1)}+O(P^{2t-\frac{1}{2}k(k+1)-c(k)}),
\end{aligned}$$

此处

$$c_1=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left|\int_0^1 e(\beta_k x^k+\cdots+\beta_1 x)\mathrm{d}x\right|^{2t}d\beta_k\cdots\mathrm{d}\beta_1$$

及

$$c_2=\sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}\sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1}\cdots\sum_{\substack{h_k=1\\(h_k,q_k)=1}}^{q_k}\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t},$$

而

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\frac{1}{q_1\cdots q_k}\sum_{x=1}^{q_1\cdots q_k}e\left(\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x\right).$$

证　1) 由于 $S(\alpha_k,\cdots,\alpha_1)$ 的周期性, 我们有

$$T(P)=\int_{-\frac{1}{\tau_1}}^{1-\frac{1}{\tau_1}}\mathrm{d}\alpha_1\cdots\int_{-\frac{1}{\tau_k}}^{1-\frac{1}{\tau_k}}|S(\alpha_k,\cdots,\alpha_1)|^{2t}\mathrm{d}\alpha_k.$$

今取

$$\tau_1=P^{\frac{1}{2}},\quad \tau_v=P^{v-\frac{1}{2}a+\sigma},\quad 2\leqslant v\leqslant k,.$$

而 $\sigma=a^3$.

由引理 7.1 可知, 对 k 维空间之每一点 $(\alpha_k,\cdots,\alpha_1)$, 我们有一有理点 $\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$ 使

$$\alpha_v=\frac{h_v}{q_v}+\beta_v,\quad (h_v,q_v)=1,\quad |\beta_v|\leqslant\frac{1}{q_v\tau_v},\quad 0<q_v\leqslant\tau_v.$$

我们现在注意所有适合条件

$$1\leqslant q_v\leqslant P^{\frac{1}{2}a-2\sigma}(2\leqslant v\leqslant k),\quad 1\leqslant q_1\leqslant P^{\frac{1}{2}-\frac{1}{2}a+\sigma}$$

的有理点. 对应于这样的一点 $\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$, 我们做一 k 维空间的间隔: 这间隔是由适合

$$|\beta_v|\leqslant\frac{1}{q_v\tau_v},\quad 1\leqslant v\leqslant k,$$

的诸 $(\alpha_k,\cdots,\alpha_1)$ 所成的. 这一间隔用 $\mathfrak{M}\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$ 来表它.

易于证明并无两个 $\mathfrak{M}$ 有公共点. 如若不然, 假定

$$\mathfrak{M}\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\quad 及\mathfrak{M}\left(\frac{h_k'}{q_k'},\cdots,\frac{h_1'}{q_1'}\right)$$

有公共点. 因为间隔不同, 所以必有一 v 使 $\frac{h_v}{q_v}\neq\frac{h_v'}{q_v'}$, 且

$$\begin{aligned}\frac{1}{q_vq_v'}\leqslant\frac{|h_vq_v'-h_v'q_v|}{q_vq_v'}&=\left|\frac{h_v}{q_v}-\frac{h_v'}{q_v'}\right|\leqslant\frac{1}{q_v\tau_v}+\frac{1}{q_v'\tau_v}\\&\leqslant\frac{2}{\tau_v}\max\left(\frac{1}{q_v},\frac{1}{q_v'}\right),\end{aligned}$$

也就是

$$\tau_v\leqslant 2\max(q_v,q_v')\leqslant\begin{cases}2P^{\frac{1}{2}a-2\sigma}, & 当v>1,\\ 2P^{\frac{1}{2}-\frac{1}{2}a+\sigma}, & 当v=1.\end{cases}$$

这是不可能的.

用 E 表示由

$$-\frac{1}{\tau_v}\leqslant\alpha_v\leqslant 1-\frac{1}{\tau_v},\quad 1\leqslant v\leqslant k,$$

中除去诸 $\mathfrak{M}$ 之后所余下的部分. 命

$$T_{(1)}=\int\underset{E}{\cdots}\int|S(\alpha_k,\cdots,\alpha_1)|^{2t}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k$$

及

$$T_{(2)}=\sum_{\mathfrak{M}}K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right),$$

$$K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=\int\underset{\mathfrak{M}}{\cdots}\int|S|^{2t}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k,$$

则

$$T(P)=T_{(1)}+T_{(2)}. \tag{1}$$

2) 命 $H=q_1\cdots q_k$ 及

$$x=H\xi+\eta,\quad \eta=1,\cdots,H,\quad -\eta/H<\xi\leqslant(P-\eta)/H,$$

则在 $\mathfrak{M}\left(\dfrac{h_1}{q_1},\cdots,\dfrac{h_k}{q_k}\right)$ 上

$$S(\alpha_k,\cdots,\alpha_1)=\sum_{\eta}W_\eta e\left(\frac{h_k}{q_k}\eta^k+\cdots+\frac{h_1}{q_1}\eta\right),$$

此处

$$W_\eta=\sum_{-\frac{\eta}{H}<\xi\leqslant\frac{P-\eta}{H}}e(\beta_k(H\xi+\eta)^k+\cdots+\beta_1(H\xi+\eta)).$$

命

$$\varphi(\xi)=\beta_k(H\xi+\eta)^k+\cdots+\beta_1(H\xi+\eta),$$

则当 P 充分大时,

$$\begin{aligned}|\varphi'(\xi)|&\leqslant\frac{kHP^{k-1}}{q_k\tau_k}+\cdots+\frac{H}{q_1\tau_1}\\&\ll\sum_{v=2}^{k}P^{(\frac12a-2\sigma)(k-2)}P^{\frac12-\frac12a+\sigma}\frac{P^{v-1}}{P^{v-\frac12a+\sigma}}+P^{(\frac12a-2\sigma)(k-1)}\frac{1}{P^{\frac12}}\\&\ll P^{-a-2\sigma(k-2)}+P^{-\frac12a-2\sigma(k-1)}=o(1),\end{aligned}$$

即当 P 充分大时, $|\varphi'(\xi)|\leqslant\dfrac12$. 故由引理 7.5.2 可知

$$W_\eta=\int_{-\eta/H}^{(P-\eta)/H}e(\varphi(z))\mathrm{d}z+O(1).$$

命 $x=P^{-1}(zH+\eta), \gamma_v=\beta_v P^v (1\leqslant v\leqslant k)$, 可得

$$W_\eta=\frac{P}{H}R+O(1),$$

此处

$$R=\int_0^1 e(\gamma_k x^k+\cdots+\gamma_1 x)\mathrm{d}x.$$

因此

$$S=B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)PR+O(H). \tag{2}$$

3) 因

$$Q\geqslant \max(q_1,\cdots,q_k)\geqslant (q_1\cdots q_k)^a=H^a,$$

故由引理 10.1 及 10.3 可知

$$B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)PR\ll PQ^{-a+\varepsilon}Z\ll PH^{-a^2+\varepsilon}Z. \tag{3}$$

又当 α 在 $\mathfrak{M}$ 上,

$$\begin{aligned}H=q_1\cdots q_k&\leqslant P^{\frac{1}{2}-\frac{1}{2}a+\sigma+(k-1)(\frac{1}{2}a-2\sigma)}\\&\leqslant P^{1-a-(2k-3)\sigma}\leqslant P^{1-a}\end{aligned}$$

及

$$\begin{aligned}Z&=\min(1,|\gamma_1|^{-a},\cdots,|\gamma_k|^{-a})\\&=\min(1,(P|\beta_1|)^{-a},\cdots,(P^k|\beta_k|)^{-a})\\&\geqslant \min(1,(P/\tau_1)^{-a},\cdots,(P^k/\tau_k)^{-a})\\&\geqslant \min(1,P^{-\frac{1}{2}a})=P^{-\frac{1}{2}a},\end{aligned}$$

所以

$$\begin{aligned}H&=H^{-a^2+\varepsilon}\cdot H^{1+a^2-\varepsilon}\\&\leqslant H^{-a^2+\varepsilon}P^{(1+a^2-\varepsilon)(1-a)}\\&\leqslant H^{-a^2+\varepsilon}P\cdot P^{-\frac{1}{2}a}\ll PH^{-a^2+\varepsilon}Z.\end{aligned} \tag{4}$$

由 (2), (3) 及 (4) 可知: 在 $\mathfrak{M}$ 上

$$S\ll PH^{-a^2+\varepsilon}Z. \tag{5}$$

4) 由 (2), (3) 及 (5) 式并简单的不等式

$$||\xi|^{2t}-|\eta|^{2t}|\leqslant 2t|\xi-\eta|(|\xi|^{2t-1}+|\eta|^{2t+1}),$$

可知

$$|S|^{2t}-\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}P^{2t}|R|^{2t}\ll H(PH^{-a^2+\varepsilon}Z)^{2t-1}.$$

在 $\mathfrak{M}\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)$ 上求积分, 可得

$$\begin{aligned}K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)=&\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}P^{2t}\int_{-q_k^{-1}\tau_k^{-1}}^{q_k^{-1}\tau_k^{-1}}\cdots\int_{-q_1^{-1}\tau_1^{-1}}^{q_1^{-1}\tau_1^{-1}}|R|^{2t}\mathrm{d}\beta_1\cdots\mathrm{d}\beta_k\\&+O(HP^{2t-1}\cdot H^{-(2t-1)a^2+\varepsilon}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}Z^{2t-1}\mathrm{d}\beta_1\cdots\mathrm{d}\beta_k).\end{aligned}$$

由引理 10.2 可知 (因为 $2t-1>k^2$)

$$\begin{aligned}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}Z^{2t-1}\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1&\leqslant P^{-\frac{1}{2}k(k+1)}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}Z^{2t-1}\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1\\&\ll P^{-\frac{1}{2}k(k+1)}.\end{aligned}$$

由此推出

$$\begin{aligned}&K\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\\=&\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}P^{2t}\int_{-q_k^{-1}\tau_k^{-1}}^{q_k^{-1}\tau_k^{-1}}\cdots\int_{-q_1^{-1}\tau_1^{-1}}^{q_1^{-1}\tau_1^{-1}}|R|^{2t}\mathrm{d}\beta_1\cdots\mathrm{d}\beta_k\\&+O(P^{2t-\frac{1}{2}k(k+1)-1}H^{1-a^2(2t-1)+\varepsilon})\\=&\left|B\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{2t}P^{2t-\frac{k}{2}(k+1)}\int_{-q_k^{-1}\tau_k^{-1}Pk}^{q_k^{-1}\tau_k^{-1}P^k}\cdots\int_{-q_1^{-1}\tau_1^{-1}P}^{q_1^{-1}\tau_1^{-1}P}|R|^{2t}\mathrm{d}\gamma_1\cdots\mathrm{d}\gamma_k\\&+O(P^{2t-\frac{1}{2}k(k+1)^{-1}H^{1-a^2}(2t-1)+\varepsilon}).\end{aligned}\tag{6}$$

5) 易见

$$\begin{aligned}&\left|\int_{-q_k^{-1}\tau_k^{-1}P^k}^{q_k^{-1}\tau_k^{-1}P^k}\cdots\int_{-q^{-1}\tau_1^{-1}P}^{q_1^{-1}\tau_1^{-1}P}|R|^{2t}\mathrm{d}\gamma_1\cdots\mathrm{d}\gamma_k-\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|R|^{2t}\mathrm{d}\gamma_1\cdots\mathrm{d}\gamma_k\right|\\\ll&\max_j M_j\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|R|^{2t-1}\mathrm{d}\gamma_1\cdots\mathrm{d}\gamma_k,\end{aligned}$$

此处 M_j 是当 $|r_j|>q_j^{-1}\tau_j^{-1}P^j$ 时 $|R|$ 的极大值. 因

$$\frac{P^j}{\tau_jq_j}\geqslant\frac{P^j}{P^{\frac{1}{2}a-2\sigma}P^{j-\frac{1}{2}a+\sigma}}=P^{\sigma},\quad 当2\leqslant j\leqslant k$$

及

$$\frac{P}{\tau_1 q_1} \geqslant \frac{P}{P^{\frac{1}{2}-\frac{1}{2}a+\sigma}P^{\frac{1}{2}}} = P^{\frac{1}{2}a-\sigma} \geqslant P^{\sigma},$$

故由引理 10.2

$$M_j \ll \max_{|\gamma_j| \geqslant P^{\sigma}} \delta_j^{-a^2} \ll P^{-a^2\sigma},$$

即得

$$\int_{-q_k^{-1}\tau_k^{-1}P^k}^{q_k^{-1}\tau_k^{-1}P^k} \cdots \int_{-q_1^{-1}\tau_1^{-1}P}^{q_1^{-1}\tau_1^{-1}P} |R|^{2t} \mathrm{d}\gamma_1 \cdots \mathrm{d}\gamma_k = c_1 + O(P^{-a^2\sigma}). \tag{7}$$

结合 (6), (7) 二式可知

$$\begin{aligned} K\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) = c_1 \left|B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)\right|^{2t} P^{2t-\frac{1}{2}k(k+1)} \\ + O(P^{2t-\frac{1}{2}k(k+1)-1}H^{1-a^2(2t-1)+\varepsilon}) \\ + O(P^{2t-\frac{1}{2}k(k+1)-a^2\sigma}H^{-2ta^2+\varepsilon}). \end{aligned} \tag{8}$$

命

$$A = \sum_{q_k \leqslant P^{\frac{1}{2}a-2\sigma}} \cdots \sum_{q_2 \leqslant P^{\frac{1}{2}a-2\sigma}} \sum_{q_1 \leqslant P^{\frac{1}{2}-\frac{1}{2}a+\sigma}} \sum_{\substack{h_1=1 \\ (h_1,q_1)=1}}^{q_1} \cdots \sum_{\substack{h_k=1 \\ (h_k,q_k=1)}}^{q_k} \left|B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)\right|^{2t}.$$

由 (8) 可知

$$\begin{aligned} T_{(2)} = c_1 A P^{2t-\frac{1}{2}k(k+1)} + O(P^{2t-\frac{1}{2}k(k+1)-1} \sum H^{1-a^2(2t-1)+\varepsilon}) \\ + O(P^{2t-\frac{1}{2}k(k+1)-a^2\sigma} \sum H^{-2ta^2+\varepsilon}). \end{aligned}$$

由于当 $t > k^2$ 时

$$\sum_q \sum_h H^{-2ta^2+\varepsilon} \leqslant \sum_{q_1,\cdots,q_k} H^{1-2ta^2+\varepsilon} \leqslant \left(\sum_{q=1}^{\infty} q^{1-2ta^2+\varepsilon}\right)^k$$

的收敛性及当 $2t < 3k^2+1$ 时

$$\sum_q \sum_h H^{1-a^2(2t-1)+\varepsilon} \leqslant \left(\sum_q q^{2-a^2(2t-1)+\varepsilon}\right)^k$$

的收敛性, 可知

$$T_{(2)} = c_1 A P^{2t-\frac{1}{2}k(k+1)} + O(P^{2t-\frac{1}{2}k(k+1)-c_4}). \tag{9}$$

假定 $t > k^2$ 只当 $k \geqslant 4$ 时成立, $2t > 3k^2+1$ 只当 $k \geqslant 5$ 时成立. 所以当 $k=3$ 及 4 时, 我们须用以下的补充才能获得 (9) 式.

当 $k=3$ 时,

$$
\begin{aligned}
&\sum_q \sum_h H^{-2ta^2+\varepsilon} \\
\leqslant &\sum_{q_1 \leqslant P^{\frac{1}{2}-\frac{1}{6}+\sigma}} \sum_{q_2 \leqslant P^{\frac{1}{6}-2\sigma}} \sum_{q_3 \leqslant P^{\frac{1}{6}-2\sigma}} (q_1q_2q_3)^{1-\frac{18}{9}+\varepsilon} \ll P^{(\frac{1}{3}+\sigma+\frac{1}{6}-2\sigma+\frac{1}{6}-2\sigma)\varepsilon}, \\
&\sum_q \sum_h H^{1-a^2(2t-1)+\varepsilon} \\
\leqslant &\sum_{q_1 \leqslant P^{\frac{1}{2}-\frac{1}{6}+\sigma}} \sum_{q_2 \leqslant P^{\frac{1}{6}-2\sigma}} \sum_{q_3 \leqslant P^{\frac{1}{6}-2\sigma}} (q_1q_2q_3)^{2-(18-1)/9+\varepsilon} \\
\ll &P^{(\frac{1}{3}+\sigma+\frac{1}{5}-2\sigma+\frac{1}{6}-2\sigma)10/9+\varepsilon} \ll P^{\frac{20}{27}+\varepsilon}
\end{aligned}
$$

及当 $k=4$ 时,

$$
\begin{aligned}
&\sum_{q_1 \leqslant P^{\frac{1}{2}-\frac{1}{8}+\sigma}} q_1^{2-(48-1)/16+\varepsilon} \left(\sum_{q \leqslant P^{\frac{1}{8}-2\sigma}} q^{2-(48-1)/16+\varepsilon} \right)^3 \\
&\ll P^{\frac{1}{16}\left(\frac{25}{64}+\frac{18}{64}\right)+\varepsilon} \leqslant P^{\frac{3}{64}+\varepsilon}.
\end{aligned}
$$

6) 今往求出 c_2 与 A 的差数. 因为 $q_1, \cdots, q_k$ 的最小公倍数 $Q > \max(q_1, \cdots, q_k)$, 所以

$$
|c_2 - A| \leqslant F \sum_{q_1=1}^{\infty} \cdots \sum_{q_k=1}^{\infty} \sum_{h_1} \cdots \sum_{h_k} \left| B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) \right|^{2t-1},
$$

此处

$$
F = \max_{Q \geqslant P^{\frac{1}{2}-\frac{1}{2}a+\sigma}} \left| B\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) \right|.
$$

由引理 10.3 知道

$$
F \ll Q^{-a+\varepsilon} \ll P^{-a(\frac{1}{2}-\frac{1}{2}a+\sigma)+\varepsilon}
$$

及由同引理 $\sum\limits_q \sum\limits_h |B|^{2t-1}$ 是收敛的 (因为 $2t > k(k+1)+1$), 所以

$$
c_2 = A + O(P^{-c_5}).
$$

和 (9) 合并起来可知

$$
T_{(2)} = c_1c_2P^{2t-\frac{1}{2}k(k+1)} + O(P^{2t-\frac{1}{2}k(k+1)-c_6}). \tag{10}
$$

7) 现在我们来讨论 $T_{(1)}$. 若 $(\alpha_k,\cdots,\alpha_1)$ 属于 E, 则必适合以下 k 个条件之一:

$$P^{\frac{1}{2}a-2\sigma}<q_v\leqslant P^{v-\frac{1}{2}a+\sigma},\quad 2\leqslant v\leqslant k,$$
$$P^{\frac{1}{2}-\frac{1}{2}\sigma+\sigma}<q_1\leqslant P^{\frac{1}{2}}.$$

如果第一类不等式之一成立, 即有一 v 使 $P^{\frac{1}{2}a-2\sigma}<q_v\leqslant P^{v-\frac{1}{2}a+\sigma}$, 则由定理 9 及引理 5.12 可知: 当 $k>11$ 时,

$$S(\alpha_k,\cdots,\alpha_1)\ll P^{1-\lambda},\quad \lambda=\frac{1}{50k^3\log k};\tag{11}$$

当 $k\leqslant 11$ 时, 由定理 9 及引理 5.11 也知此式真实.

如果不适合第一类的不等式, 则所讨论的情况适合了引理 10.5 的假定, 得出

$$S\ll P^{1-\sigma}\ll P^{1-\lambda},\quad \lambda=\frac{1}{50k^3\log k}.$$

换言之, 在 E 上常有 (11) 式

8) 现在我们将证明

$$T_{(1)}\ll P^{2t-\frac{1}{2}k(k+1)-c_7}.\tag{12}$$

8.1) 假定 $k<11$, 则由定理 7 及 (11) 式

$$\begin{aligned}T_{(1)}&\ll P^{2(1-\lambda)}\int_0^1\cdots\int_0^1|S|^{2t-2}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\&\ll P^{2t-\frac{1}{2}k(k+1)-c_7}.\end{aligned}$$

8.2) 今假定 $k\geqslant 11$, 由定理 5 取 $t=t_1+k^2$, 则

$$\begin{aligned}T_{(1)}&\ll P^{2k^2(1-\lambda)}\int_0^1\cdots\int_0^1|S|^{2t_1}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\&\ll P^{2k^2(1-\lambda)+2t_1-\frac{1}{2}k(k+1)+\frac{1}{2}k(k+1)(1-a)^l+\varepsilon}\\&\ll P^{2t-\frac{1}{2}k(k+1)-c_5},\end{aligned}$$

此处

$$c_5=\frac{1}{25k\log k}-\frac{1}{2}k(k+1)(1-a)^l-\varepsilon.$$

取

$$l=\left[\frac{\log(13k^2(k+1)\log k)}{-\log(1-a)}\right]+1.$$

这保证了 $c_5>0$. 同时, 当 $k\geqslant 11$ 时,

$$l<\frac{3\log k+\log\log k+\log(1+a)+\log 13}{-\log(1-a)}+1$$

$$< k(3\log k + \log\log k + \log(1+a) + \log 13)\left(1 - \frac{1}{3}a\right) + 1,$$

所以

$$\begin{aligned} t = t_1 + k^2 &\leqslant lk + \frac{1}{4}(k^2+k+2) + k^2 \\ &\leqslant k^2(3\log k + \log\log k + \log(1+a) + \log 13)\left(1 - \frac{1}{3}a\right) \\ &\quad + \frac{5}{4}(k^2+k) + \frac{1}{2} \\ &< k^2\left(3\log k + \log\log k + \log\frac{12}{11} + \log 13 + \frac{5}{4}\right) \\ &\quad - k\left(\log k - \frac{5}{4} - \frac{1}{2}a\right) \\ &< k^2(3\log k + \log\log k + 4) - 11. \end{aligned}$$

由 (1), (10) 及 (12) 证出定理 15.

注意：我们并未算出定理 15 中 $k=2$ 的部分. 读者不难自己补出其证明. 更进一步, 在 $k=2$ 时, 常数 c_1 及 c_2 都可能算出来.

§10.4　定理 16 的叙述

定理 16　命 k 表一 $\geqslant 2$ 的整数. s 是一 $\geqslant s_0$ 的整数, 此处 s_0 的定义如次

k	2	3	4	5	6	7	8	9	10	$\geqslant 11$
s_0	7	19	49	113	243	417	675	1083	1773	$2k^2(3\log k + \log\log k + 4) - 21$

命 $I(N_k, \cdots, N_1)$ 代表下列方程组

$$\left.\begin{aligned} p_1 + p_2 + \cdots + p_s &= N_1, \\ p_1^2 + p_2^2 + \cdots + p_s^2 &= N_2, \\ &\cdots\cdots \\ p_1^k + p_2^k + \cdots + p_s^k &= N_k \end{aligned}\right\} \tag{1}$$

的素数解 $p_1, \cdots, p_s$ 的组数. 命 $N_k^a = P$. 则 (1) 式的解组数可以表成

$$I(N_k, \cdots, N_1) = \frac{b_1 P^{s-\frac{1}{2}k(k+1)}\mathfrak{S}(N_k, \cdots, N_1)}{L^s} + O\left(\frac{P^{s-\frac{1}{2}k(k+1)}}{L^{s+1}}\log L\right),$$

此处

$$b_1=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_0^1 e(\gamma_k x^k+\cdots+\gamma_1 x)\mathrm{d}x\right)^s e\left(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\right)\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1,$$

$$\mathfrak{S}(N_k,\cdots,N_1)=\sum_{q_1,\cdots,q_k=1}^{\infty}A(q_k,\cdots,q_1),$$

$$A(q_k,\cdots,q_1)=\sum_{h_1,\cdots,h_k}{}' T^s e\left(-\frac{h_k}{q_k}N_k-\cdots-\frac{h_1}{q_1}N_1\right),$$

此处 $h_1,\cdots,h_k$ 分别经过一个既约剩余系, mod $q_1,\cdots$, mod q_k, 且

$$T=\frac{1}{\varphi(Q)}\sum_x{}' e\left(\frac{h_k}{q_k}x^k+\cdots+\frac{h_1}{q_1}x\right),$$

此处 Q 是 $q_1,\cdots,q_k$ 的最小公倍数, 而 x 则经过一既约剩余系, mod Q.

§10.5 定理的证明

1) 命

$$S(\alpha_k,\cdots,\alpha_1)=\sum_{p\leqslant P}e(f(p)),\quad f(x)=\alpha_k x^k+\cdots+\alpha_1 x,$$

则

$$\begin{aligned}I(N_k,\cdots,N_1)&=\int_0^1\mathrm{d}\alpha_1\cdots\int_0^1 S^s(\alpha_k,\cdots,\alpha_1)e(-N_k\alpha_k-\cdots-N_1\alpha_1)\mathrm{d}\alpha_k\\&=\int_{-\tau_1^{-1}}^{-1-\tau_1^{-1}}\mathrm{d}\alpha_1\cdots\int_{-\tau_k^{-1}}^{1-\tau_k^{-1}}S^s(\alpha_k,\cdots,\alpha_1)e(-N_k\alpha_k-\cdots-N_1\alpha_1)\mathrm{d}\alpha_k,\end{aligned}$$

此处 $\tau_v=P^vL^{-\sigma_v}$ 及

$$\sigma_v\geqslant 2^{6k+1}(\sigma_k+\cdots+\sigma_{v+1}+s_1+1),\quad \sigma_k>2k^2,$$

而 s_1 则是一任意的正整数.

对于 $(-\tau_v^{-1},1-\tau_v^{-1})$ 中的任意一个 α_v, 可有二整数 h_v 及 q_v 使

$$\alpha_v-\frac{h_v}{q_v}=\beta_v,\quad |\beta_v|\leqslant\frac{1}{q_v\tau_v},\quad (h_v,q_v)=1,\quad 0<q_v\leqslant\tau_v.$$

因之, 所有的点 $(\alpha_k,\cdots,\alpha_1)$ 必定落在一个形如

$$\left|\alpha_v-\frac{h_v}{q_v}\right|\leqslant\frac{1}{q_v\tau_v},\quad 1\leqslant v\leqslant k$$

的域内.

我们把所有这样的域分为下列几类:

1°. 其中的 q_k 适合于 $L^{\sigma_k} \leqslant q_k \leqslant \tau_k$ 者, 用 m_k 表示它们中间的一个;

2°. q_k 适合于 $0 < q_k < L^{\sigma_k}$ 及 q_{k-1} 适合于 $L^{\sigma_{k-1}} \leqslant q_{k-1} \leqslant \tau_{k-1}$ 者, 用 m_{k-1} 表示它们中间的一个;

....

v°. 如果 $0 < q_k < L^{\sigma_k}, \cdots, 0 < q_{k-v+2} < L^{\sigma_{k-v+2}}$, 但 $L^{\sigma_{k-v+1}} \leqslant q_{k-v+1} \leqslant \tau_{k-v+1}$, 则用 m_{k-v+1} 表示它们中间的一个;

....

k°. 如果 $0 < q_k < L^{\sigma_k}, \cdots, 0 < q_2 < L^{\sigma_2}$, 但 $L^{\sigma_1} < q_1 \leqslant \tau_1$, 则用 m_1 表示它们中的一个;

$(k+1)^\circ$. 适合于 $0 < q_v < L^{\sigma_v}, 1 \leqslant v \leqslant k$ 的域用 $\mathfrak{M} = \mathfrak{M}\left(\dfrac{h_k}{q_k}, \cdots, \dfrac{h_1}{q_1}\right)$ 来表它.

易于证明: 当 P 充分大时, 并无两个 $\mathfrak{M}$ 有公共点. 用 $\mathfrak{N}$ 代表所有的 $\mathfrak{M}$ 之外的点的集合, 则得

$$I(N_k, \cdots, N_1) = \left(\sum_{\mathfrak{M}} \int_{\mathfrak{M}} + \int_{\mathfrak{N}}\right) S^s e(-\alpha_k N_k - \cdots - \alpha_1 N_1) \mathrm{d}\alpha_k \cdots \mathrm{d}\alpha_1.$$

2) **引理 10.6**　命

$$S^*(\beta_k, \cdots, \beta_1) = \int_2^p \frac{e(\Psi(x))}{\log x} \mathrm{d}x, \quad \Psi(x) = \beta_k x^k + \cdots + \beta_1 x,$$

则在 $\mathfrak{M}\left(\dfrac{h_k}{q_k}, \cdots, \dfrac{h_1}{q_1}\right)$ 上

$$S(\alpha_k, \cdots, \alpha_1) = T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) \frac{1}{\varphi(Q)} S^*(\beta_k, \cdots, \beta_1) + O(P\mathrm{e}^{-c_1\sqrt{L}}),$$

此处

$$T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) = \sum_{\substack{x=1 \\ (x,Q)=1}}^{Q} e\left(\frac{h_k}{q_k} x^k + \cdots + \frac{h_1}{q_1} x\right),$$

而 Q 则是 $q_k, \cdots, q_1$ 的最小公倍数.

证　显然有 $Q < L^{\sigma_1 + \cdots + \sigma_k}$. 命

$$S_m = \sum_{2 \leqslant p \leqslant m} e\left(\frac{h_k}{q_k} p^k + \cdots + \frac{h_1}{q_1} p\right), \quad S_1 = 0.$$

则由引理 7.14,

$$S_m = \sum_{\substack{x=1\\(x,Q)=1}}^{Q} e\left(\frac{h_k}{q_k}x^k + \cdots + \frac{h_1}{q_1}x\right) \sum_{\substack{p\leqslant m\\ p\equiv x(Q)}} 1 + O(Q^\varepsilon)$$
$$= T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) \frac{\operatorname{li}m}{\varphi(Q)} + O(P\mathrm{e}^{-c_2\sqrt{L}}).$$

我们有

$$S(\alpha_k, \cdots, \alpha_1) = \sum_{2\leqslant m\leqslant P} (S_m - S_{m-1}) e(\Psi(m))$$
$$= \sum_{2\leqslant m\leqslant P} S_m(e(\Psi(m)) - e(\Psi(m+1))) + S_P e(\Psi(P+1))$$
$$= \frac{T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)}{\varphi(Q)} \left(\sum_{2\leqslant m\leqslant P} \operatorname{li}m(e(\Psi(m)) - e(\Psi(m+1)))\right.$$
$$\left. + \operatorname{li}Pe(\Psi(P+1))\right) + O(P\mathrm{e}^{-c_3\sqrt{L}}),$$

这是因为

$$P\mathrm{e}^{-c_2\sqrt{L}} \left(\sum_{2\leqslant m\leqslant P} |e(\Psi(m)) - e(\Psi(m+1))| + 1\right)$$
$$\ll P\mathrm{e}^{-c_2\sqrt{L}} L^{\sigma_1+\sigma_2+\cdots+\sigma_k} \ll P\mathrm{e}^{-c_4\sqrt{L}}.$$

又

$$\sum_{2\leqslant m\leqslant P} \operatorname{li}m(e(\Psi)(m) - e(\Psi(m+1))) + \operatorname{li}Pe(\Psi(P+1))$$
$$= \sum_{3\leqslant m\leqslant P} e(\Psi(m)) \int_{m-1}^{m} \frac{\mathrm{d}x}{\log x}$$
$$= \sum_{3\leqslant m\leqslant P} \int_{m-1}^{m} \frac{e(\Psi x)}{\log x} \mathrm{d}x + O(L^{\sigma_1+\cdots+\sigma_k})$$
$$= S^*(\beta_k, \cdots, \beta_1) + O(L^{\sigma_1+\cdots+\sigma_k}),$$

由此即得出本引理.

引理 10.7　命 $\gamma_k, \cdots, \gamma_1$ 代表实数, $\Phi(y) = \gamma_k y^k + \cdots + \gamma_1 y$. 又命 $W =$

$\prod_{v=1}^{k}\delta_v^{-a^2}, \delta_v=\max(1,|\gamma_v|)$, 则

$$\int_{2/P}^{1}\frac{e(\Phi(y))}{\log yP}\mathrm{d}y=\frac{1}{L}\int_{0}^{1}e(\Phi(y))\mathrm{d}y+O\left(\frac{\log L}{L^2}W\right),$$

因而 (引理 10.2)

$$\int_{2/P}^{1}\frac{e(\Phi(y))}{\log yP}\mathrm{d}y\ll\frac{W}{L}.$$

证　由第二中值定理及引理 10.2 可得

$$\begin{aligned}&\frac{1}{L}\int_{0}^{1}e(\Phi(y))\mathrm{d}y-\int_{2/P}^{1}\frac{e(\Phi(y))}{\log yP}\mathrm{d}y\\&=\frac{1}{L}\int_{0}^{L^{-8}}e(\Phi(y))\mathrm{d}y-\int_{2/P}^{L^{-8}}\frac{e(\Phi(y))}{\log y+L}\mathrm{d}y+\frac{1}{L}\int_{L^{-8}}^{1}\frac{\log y}{\log y+L}e(\Phi(y))\mathrm{d}y\\&\ll L^{-8}\prod_{v=1}^{k}\max(1,L^{-8v}|\gamma_v|)^{-a^2}+\frac{\log L}{L^2}W\\&\ll L^{-4(1-a)}W+\frac{\log L}{L^2}W\\&\ll WL^{-2}\log L.\end{aligned}$$

3) **引理 10.8.**　在 $\mathfrak{N}$ 上

$$S(\alpha_k,\cdots\alpha_1)\ll PL^{-s_1}.$$

证　假定 α 在 m_n 上. 命

$$S_0=S\left(\frac{h_k}{q_k},\cdots,\frac{h_n}{q_n},\alpha_{n-1},\cdots,\alpha_1\right).$$

命 Q_n 代表 $q_k,\cdots,q_{n+1}$ 的最小公倍数. 则 $Q_n\ll L^{\sigma_k+\cdots+\sigma_{n+1}}$. 由定理 10, 我们有

$$\begin{aligned}|S_0|&\leqslant\sum_{t=1}^{Q_n}\left|\sum_{\substack{p\leqslant P\\p\equiv t(\mathrm{mod}Q_n)}}e\left(\frac{h_n}{q_n}p^n+\cdots+\alpha_1p\right)\right|\\&\ll PL^{-s_1-\sigma_k-\cdots-\sigma_{n+1}}\end{aligned}$$

(由于 $\sigma_n\geqslant2^{6k+1}(\sigma_h+\cdots+\sigma_{n+1}+s_1+1)$).

命

$$S(m)=\sum_{2\leqslant p\leqslant m}e\left(\frac{h_k}{q_k}p^k+\cdots+\frac{h_n}{q_n}p^n+\alpha_{n-1}p^{n-1}+\cdots+\alpha_1p\right),$$

即得出

$$S(\alpha_k,\cdots,\alpha_1)=\sum_{2\leqslant m\leqslant P}(S(m)-S(m-1))e(\Psi_1(m))$$
$$=\sum_{2\leqslant m\leqslant P}S(m)(e(\Psi_1(m))-e(\Psi_1(m+1)))+S(P)e(\Psi_1(P+1)),$$

此处

$$\Psi_1(x)=\beta_k x^k+\cdots+\beta_n x^n.$$

故得出

$$S(\alpha_k,\cdots,\alpha_1)\ll PL^{-s_1-\sigma_k-\cdots-\sigma_{n+1}}\sum_{2\leqslant m\leqslant P}(P^{-1}(L^{\sigma_k}+\cdots+L^{\sigma_{n+1}})+P^{-1})$$
$$+PL^{-s_1-\sigma_k-\cdots-\sigma_{n+1}}\ll PL^{-s_1}.$$

4) 当 $k\geqslant 3$, 由定理 15 及引理 10.8 得出

$$\int\underset{\mathfrak{R}}{\cdots}\int|S(\alpha_k,\cdots,\alpha_1)|^s\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1$$
$$\ll(PL^{-s_1})^{s-s_0+1}\int\underset{\mathfrak{R}}{\cdots}\int|S(\alpha_k,\cdots,\alpha_1)|^{s_0-1}\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1$$
$$\ll P^{s-\frac{1}{2}k(k+1)}L^{-s_1}.$$

当 $k=2$, 则由定理 7(定理 B_2'), 得出

$$\iint_{\mathfrak{R}}|S(\alpha_2,\alpha_1)|^7\mathrm{d}\alpha_2\mathrm{d}\alpha_1\ll PL^{-s_1}\int_0^1\int_0^1|S(\alpha_2,\alpha_1)|^6\mathrm{d}\alpha_2\mathrm{d}\alpha_1$$
$$\ll P^{s-\frac{1}{2}k(k+1)}L^{-s_1+3}.$$

5) **引理 10.9.** 若 $g\geqslant k^2+1$, 则

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|S^*(\beta_k,\cdots,\beta_1)|^g\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1\ll P^{g-\frac{1}{2}k(k+1)}L^{-g}.$$

证　左边的积分是

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left|\int_2^P\frac{e(\beta_k x^k+\cdots+\beta_1 x)}{\log x}\mathrm{d}x\right|^g\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1.$$

命 $x=Py,\beta_v=\gamma_v P^{-v}$, 则此积分等于

$$P^{g-\frac{1}{2}k(k+1)}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left|\int_{2/P}^1\frac{e(\gamma_k y^k+\cdots+\gamma_1 y)}{\log yP}\mathrm{d}y\right|^g\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1$$

$$\ll P^{g-\frac{1}{2}k(k+1)}L^{-g}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}W^g\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1.$$

过程中用了引理 10.7. 由引理 10.2 即得出本引理.

引理 10.10　当 $s>k(k+1)$ 时, $\mathfrak{S}(N_k,\cdots,N_1)$ 绝对收敛.

证明一如引理 10.3, 但引用第一章推论 1.3 以代替定理 1.

6) 今仍利用简单的不等式

$$|\xi^s-\eta^s|\leqslant s|\xi-\eta|(|\xi|^{s-1}+|\eta|^{s-1}).$$

由引理 10.6 得出

$$\begin{aligned}&\sum_{\mathfrak{M}}\int\underset{\mathfrak{M}}{\cdots}\int S^s(\alpha_k,\cdots,\alpha_1)e(-N_k\alpha_k-\cdots-N_1\alpha_1)\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1\\&-\sum_{\mathfrak{M}}\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s e\left(-\frac{N_kh_k}{q_k}-\cdots-\frac{N_1h_1}{q_1}\right)\\&\times\int\underset{\mathfrak{M}}{\cdots}\int S^{*s}(\beta_k,\cdots,\beta_1)e(-N_k\beta_k-\cdots-N_1\beta_1)\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1\\&\ll P\mathrm{e}^{-c_1\sqrt{L}}\left(\int_0^1\cdots\int_0^1|S(\alpha_k,\cdots,\alpha_1)|^{s-1}\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1\right.\\&\quad\left.+\sum_q\sum_h Q^{-(s-1)a+\varepsilon}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|S^*(\beta_k,\cdots,\beta_1)|^{s-1}\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1\right)\\&\ll P^{s-\frac{1}{2}k(k+1)}\mathrm{e}^{-c_1\sqrt{L}}.\end{aligned}$$

在获得此式的过程中我们根据了以下的一些事实：由定理 15 有

$$\int_0^1\cdots\int_0^1|S(\alpha_k,\cdots,\alpha_1)^{s-1}\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1\ll P^{s-1-\frac{1}{2}k(k+1)}.$$

(当 $k=2$ 时需略加修正, 但这种修正并不困难). 又由引理 10.9,

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}|S^*|^{s-1}\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1\ll P^{s-1-\frac{1}{2}k(k+1)}$$

及

$$\sum_q\sum_h Q^{-(s-1)a+\varepsilon}\leqslant\sum_q(q_1\cdots q_k)^{1-(s-1)a^2+\varepsilon}=O(L^{c_5})$$

(因为 $q_1,\cdots,q_k$ 的最小公倍数 $\geqslant(q_1\cdots q_k)^a$).

7) 我们有

$$\left(\sum_{\mathfrak{M}} - \sum_{q_k \leqslant L^{\frac{1}{2}\sigma_k}} \cdots \sum_{q_1 \leqslant L^{\frac{1}{2}\sigma_1}} \sum_{h_1}{}' \cdots \sum_{h_k}{}'\right) \left(\frac{T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s e\left(-\frac{N_k h_k}{q_k} - \cdots - \frac{N_1 h_1}{q_1}\right)$$

$$\times \int \underset{\mathfrak{M}}{\cdots} \int S^{*s} e(-N_k\beta_k - \cdots - N_1\beta_1) \mathrm{d}\beta_k \cdots \mathrm{d}\beta_1$$

$$\ll M \sum_{q_k=1}^{\infty} \cdots \sum_{q_1=1}^{\infty} \sum_{h_1}{}' \cdots \sum_{h_k}{}' \left|\frac{T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)}{\varphi(Q)}\right|^{s-1} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} |S^*|^s \mathrm{d}\beta_k \cdots \mathrm{d}\beta_1, \tag{1}$$

此处

$$M = \max_{v} \max_{q_v \geqslant L^{\frac{1}{2}\sigma_v}} \left|\frac{T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right)}{\varphi(Q)}\right|.$$

由第一章推理 1.3 易知

$$\begin{aligned} M &\ll \max_{v} \max_{q_v \geqslant L^{\frac{1}{2}\sigma_v}} Q^{-a+\varepsilon} \ll \max_{v} \max_{q_v \geqslant L^{\frac{1}{2}\sigma_v}} q_v^{-a+\varepsilon} \\ &\ll L^{-\frac{1}{2}a\sigma_k+\varepsilon} \ll L^{-1} \end{aligned}$$

及由引理 10.10, (1) 式中的级数是收敛的; 再由引理 10.9, (1) 式中的积分部分是 $\leqslant P^{s-\frac{1}{2}k(k+1)}L^{-s}$. 故知 (1) 式之右边 $\leqslant P^{s-\frac{1}{2}k(k+1)}L^{-s-1}$.

8) 当 $q_v \leqslant L^{\frac{1}{2}\sigma_v}, 1 \leqslant v \leqslant k$, 我们有

$$\begin{aligned} &\left(\int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} - \int \underset{\mathfrak{M}}{\cdots} \int\right) |S^*|^s \mathrm{d}\beta_1 \cdots \mathrm{d}\beta_k \\ &\ll M \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} |S^*|^{s-1} \mathrm{d}\beta_1 \cdots \mathrm{d}\beta_k, \end{aligned} \tag{2}$$

此处

$$M = \max_{v} \max_{|\beta_v| > q_v^{-1} P^{-v} L^{-\sigma_v}} |S^*|.$$

由引理 10.7 及

$$|\gamma_v| = P^v |\beta_v| > q_v^{-1} L^{\sigma_v} \geqslant L^{\frac{1}{2}\sigma_v},$$

可知

$$M \ll \frac{P}{L} \max_{v} \max_{|\gamma_v| > L^{\frac{1}{2}\sigma_v}} \min(1, |\gamma_v|^{-a^2}) \ll \frac{P}{L} L^{-\frac{1}{2}a^2\sigma_k} \ll PL^{-2}.$$

再用引理 10.9, (2) 式的右边 $\ll P^{s-\frac{1}{2}k(k+1)}L^{-s-1}$. 联合 (1) 及 (2), 可以得到

$$\sum_{\mathfrak{M}}\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s e\left(-\frac{h_k}{q_k}N_k-\cdots-\frac{h_1}{q_1}N_1\right)\int\underset{\mathfrak{M}}{\cdots}\int S^{*s}(\beta_k,\cdots,\beta_1)$$
$$\times e(-N_k\beta_k-\cdots-N_1\beta_1)\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1$$
$$=\sum_{q_k\leqslant L^{\frac{1}{2}\sigma_k}}\cdots\sum_{q_1\leqslant L^{\frac{1}{2}\sigma_1}}\sum_{h_k}{}'\cdots\sum_{h_1}{}'\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s e\left(-\frac{h_k}{q_k}N_k-\cdots-\frac{h_1}{q_1}N_1\right)$$
$$\times\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}S^{*s}(\beta_k,\cdots,\beta_1)e(-\beta_kN_k-\cdots-\beta_1N_1)\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1$$
$$+O(P^{s-\frac{1}{2}k(k+1)L^{-s-1}}).\tag{3}$$

9) 当 $k\geqslant 3$, 我们有

$$\mathfrak{S}(N_k,\cdots,N_1)-\sum_{q_k\leqslant L^{\frac{1}{2}\sigma_k}}\cdots\sum_{q_1\leqslant L^{\frac{1}{2}\sigma_1}}\sum_{h_k}{}'\cdots\sum_{h_1}{}'\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s$$
$$\times e\left(-\frac{h_k}{q_k}N_k-\cdots-\frac{h_1}{q_1}N_1\right)$$
$$\ll M\sum_{q_k=1}^{\infty}\cdots\sum_{q_1=1}^{\infty}\sum_{h_1}{}'\cdots\sum_{h_k}{}'\left|\frac{1}{\varphi(Q)}T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|^{s-1},\tag{4}$$

此处

$$M=\max_{v}\max_{q_v\geqslant L^{\frac{1}{2}\sigma_v}}\left|\frac{1}{\varphi(Q)}T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)\right|.$$

由 $M\ll L^{-\frac{1}{2}a\sigma_k+\epsilon}\ll L^{-1}$ 及引理 10.10, 所以 (4) 式的右边 $\ll L^{-1}$. (当 $k=2$, 须加修改).

因此得出

$$\sum_{\mathfrak{M}}\left(\frac{T\left(\frac{h_k}{q_k},\cdots,\frac{h_1}{q_1}\right)}{\varphi(Q)}\right)^s e\left(-\frac{h_kN_k}{q_k}-\cdots-\frac{h_1N_1}{q_1}\right)$$
$$\times\int\underset{\mathfrak{M}}{\cdots}\int S^{*s}e(-N_k\beta_k-\cdots-N_1\beta_1)\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1$$
$$=\mathfrak{S}(N_k,\cdots,N_1)\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}S^{*s}(\beta_k,\cdots,\beta_1)e(-\beta_kN_k-\cdots-\beta_1N_1)\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1$$

$+O(P^{s-\frac{1}{2}k(k+1)}L^{-s-1}).$

10) 我们有

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}S^{*s}(\beta_k,\cdots,\beta_1)e(-N_k\beta_k-\cdots-N_1\beta_1)\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1$$
$$=P^{s-\frac{1}{2}k(k+1)}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_{2/P}^{1}\frac{e(\gamma_kx^k+\cdots+\gamma_1x)}{\log xP}\mathrm{d}x\right)^s$$
$$e\left(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\right)\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1.$$

由引理 10.7,

$$\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_{2/P}^{1}\frac{e(\gamma_kx^k+\cdots+\gamma_1x)}{\log xP}\mathrm{d}x\right)^s e\left(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\right)\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1$$
$$=\frac{1}{L^s}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_{0}^{1}e(\gamma_kx^k+\cdots+\gamma_1x)\mathrm{d}x\right)^s e\left(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\right)\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1$$
$$+O\left(\frac{\log L}{L^{s+1}}\right)\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}W^s\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1=\frac{b_1}{L^s}+O\left(\frac{\log L}{L^{s+1}}\right).$$

所以最后获得

$$\sum_{\mathfrak{M}}\int_{\mathfrak{M}}S^s(\alpha_k,\cdots,\alpha_1)e(-\alpha_kN_k-\cdots-\alpha_1N_1)\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1$$
$$=b_1\mathfrak{S}(N_k,\cdots N_1)\frac{P^{s-\frac{1}{2}k(k+1)}}{L^s}+O\left(\frac{P^{s-\frac{1}{2}k(k+1)}}{L^{s+1}}\log L\right),$$

此处

$$b_1=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_{0}^{1}e(\gamma_kx^k+\cdots+\gamma_1x)\mathrm{d}x\right)^s e\left(-\frac{N_k}{P^k}\gamma_k-\cdots-\frac{N_1}{P}\gamma_1\right)\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1.$$

因此得出本引理.

如果 $b_1\geqslant b>0$ 及 $\mathfrak{S}(N_k,\cdots,N_1)\geqslant c>0$(此处 b 及 c 与 N 无关), 则可以得出：当 N_k 充分大时, 不定方程

$$\sum_{v=1}^{s}p_v^h=N_h,\quad 1\leqslant h\leqslant k,$$

有素数解 $p_1,\cdots,p_s$. 保证 $b_1\geqslant b>0$ 的条件将称为 “正可解条件”, 而保证 $c_1\geqslant c>0$ 的条件则称为 “同余可解条件”.

§10.6 附　录

在本章的开始就已说明：为了避免烦琐起见把 $k=2$ 的情况除外. 由以上的方法略加修改, 我们不难获得本章定理对 $k=2$ 时的真实性. 不但如此, 在本节中我们还进一步具体地算出正可解条件的积分, 和同余可解条件的奇异级数. 为了不太冗长, 我们将略去许多复杂的计算.

1) 正可解条件的研究.

在计算中我们要用到下面几个结果:

1°. 命 $\delta>0, \alpha>0$. 有不等式

$$(\delta-x_1-\cdots-x_n)^2+\alpha(x_1^2+\cdots+x_n^2) \geqslant \frac{\alpha}{n+\alpha}\delta^2. \tag{1}$$

等号仅当 $x_1=\cdots=x_n=\dfrac{\delta}{n+\alpha}$ 时成立.

2°. 命 $a<0$ 及 $b>0$. 又命 $f(x)$ 是一 (a,b) 中的连续函数. 则

$$\lim_{w\to\infty}\int_a^b \frac{\sin 2\pi x\omega}{\pi x} f(x)\mathrm{d}x = f(0). \tag{2}$$

3°. 命 $Q(x_1,\cdots,x_n)=\sum\limits_{i,j=1}^{n} q_{ij}x_ix_j$ 代表一定正二次型, 它的行列式用 $|Q|$ 代表它. 又 $L(x_1,\cdots,x_n)$ 是一齐次线性式, 同时 L 也表示其系数所成的矢量. 又命 $A>0$. 命 R 表一超椭圆体的内部:

$$A+2L(x_1,\cdots,x_n)-Q(x_1,\cdots,x_n)>0.$$

方阵

$$\begin{pmatrix} A & L \\ L' & -Q \end{pmatrix}$$

的行列式的绝对值以 $|\Delta|$ 表它. L' 表由 L 的系数自上而下排成的列. 则

$$\int\underset{R}{\cdots}\int \frac{\mathrm{d}x_1\cdots\mathrm{d}x_n}{\sqrt{A+2L(x_1,\cdots,x_n)-Q(x_1,\cdots,x_n)}} = |Q|^{-\frac{1}{2}n}|\Delta|^{\frac{1}{2}(n-1)}\frac{\pi^{\frac{1}{2}(n+1)}}{\Gamma\left(\dfrac{1}{2}(n+1)\right)}. \tag{3}$$

4°. 命 Δ_n 是二次型 $(x_1+\cdots+x_n)^2+2x_1^2+\cdots+2x_n^2$ 的行列式, 则 $\Delta_n=(n+2)2^{n-1}$. 又命 U 是二次型

$$ux_0^2+2vx_0(x_1+\cdots+x_n)+(x_1+\cdots+x_n)^2+2x_1^2+\cdots+2x_n^2$$

的行列式, 则

$$U=2^{n-1}((n+2)(u+v^2)-2(n+1)v^2).$$

现在研究与正可解有关的定积分

$$J(\delta)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left(\int_0^1 \mathrm{e}^{2\pi\mathrm{i}(a_2x^2+a_1x)}\mathrm{d}x\right)^s \mathrm{e}^{-2\pi\mathrm{i}(a_2+a_1\delta)}\mathrm{d}\alpha_2\mathrm{d}\alpha_1.$$

把它当做

$$J_w(\delta)=\int_{-\omega}^{\omega}\int_{-\omega}^{\omega}\left(\int_0^1 \mathrm{e}^{2\pi\mathrm{i}(a_2x^2+a_1x)}\mathrm{d}x\right)^s \mathrm{e}^{-2\pi\mathrm{i}(a_2+a_1\delta)}\mathrm{d}\alpha_2\mathrm{d}\alpha_1.$$

的极限. 命

$$X=x_1^2+\cdots+x_s^2-1,\quad Y=x_1+\cdots+x_s-\delta,$$

则

$$\begin{aligned}J_\omega(\delta)&=\int_0^1\cdots\int_0^1\frac{\sin 2\pi X\omega}{\pi X}\frac{\sin 2\pi Y\omega}{\pi Y}\mathrm{d}x_1\cdots\mathrm{d}x_s\\&=2\int_0^1\underset{x_1\geqslant x_2}{\cdots}\int_0^1\frac{\sin 2\pi X\omega}{\pi X}\frac{\sin 2\pi Y\omega}{\pi Y}\mathrm{d}x_1\cdots\mathrm{d}x_s.\end{aligned}$$

现有

$$J_\omega(\delta)=\int\int\frac{\sin 2\pi X\omega}{\pi X}\frac{\sin 2\pi Y\omega}{\pi Y}\mathrm{d}X\mathrm{d}Y\int_0^1\cdots\int_0^1\frac{\mathrm{d}x_3\cdots\mathrm{d}x_s}{x_1-x_2}.$$

由 2° 可得

$$\begin{aligned}J(\delta)=\lim_{\omega\to\infty}J_\omega(\delta)&=\underset{\substack{x_1^2+\cdots+x_s^2=1\\x_1+\cdots+x_s=\delta\\x_1>x_2}}{\int\cdots\int}\frac{\mathrm{d}x_3\cdots\mathrm{d}x_s}{x_1-x_2}\\&=\int\underset{\mathfrak{D}}{\cdots}\int\frac{\mathrm{d}x_3\cdots\mathrm{d}x_s}{\sqrt{2(1-x_3^2-\cdots-x_s^2)-(\delta-x_3-\cdots-x_s)^2}}.\end{aligned}$$

这积分所经过的范围 $\mathfrak{D}$ 受下列一些条件的限制:

$$2(1-x_3^2-\cdots-x_s^2)\geqslant(\delta-x_3-\cdots-x_s)^2,\tag{4}$$

$$(\delta-x_3-\cdots-x_s)^2\geqslant 1-x_3^2-\cdots-x_s^2,\tag{5}$$

$$x_v\geqslant 0.\tag{6}$$

由 1° 可知 $(\delta-x_3-\cdots-x_s)^2+2(x_3^2+\cdots+x_s^2)\geqslant 2\delta^2/s$. 根据此式可知: 若 $s<\delta^2$, 则 (4) 式决不可能; 即当 $s<\delta^2$ 时, $J(\delta)=0$. 又由 (6) 式, 我们可以看出, 在积分范围内 $x_3+\cdots+x_s\leqslant\delta$. 若 $\delta<1$, 则由

$$1-x_3^2-\cdots-x_s^2\geqslant 1-(x_3+\cdots+x_s)^2\geqslant(1-x_3-\cdots-x_s)^2\geqslant(\delta-x_3-\cdots-x_s)^2,$$

(5) 式成为不可能. 因为当 $\delta \leqslant 1$ 时, $J(\delta)=0$.

今假定 $s \geqslant \delta^2$. (4) 表示在超椭圆体 $2(1-x_3^2-\cdots-x_s^2)=(\delta-x_3-\cdots-x_s)^2$ 之内, 而 (5) 表示在超椭圆体 $1-x_3^2-\cdots-x_s^2=(\delta-x_3-\cdots-x_s)^2$ 之外. 又易见凡第一个超椭圆体上之点一定在第二个超椭圆体之外, 而第二个超椭圆体上之点一定在第一个超椭圆体之内. 换言之, 第一个超椭圆体一定包有第二个超椭圆体. 这两个超椭圆体的共同部分 $x_3+\cdots+x_s=\delta, x_3^2+\cdots+x_s^2=1$ 是一低于 $s-2$ 维的域, 所以有一块有正 n 维容积的部分存在适合 (4), (5) 及 (6). 即得.

引理 10.11　命 $s \geqslant 3$. 若 $s \geqslant \delta^2 > 1$, 则 $J(\delta)>0$.

如果我们再假定 $\delta^2 > s-1$, 则我们还可以算出函数 $J(\delta)$. 因为不等式 (5) 可以取消: 即当 $\delta^2 > s-1$, 则由 1°, 可知

$$x_3^2+\cdots+x_s^2+(\delta-x_3-\cdots-x_s)^2 \geqslant \frac{1}{s-1}\delta^2 > 1,$$

即 (5) 自然地适合了.

又 (6) 式也可以取消: 由 (4) 已知 $x_v \leqslant 1$, 如果 $x_3+\cdots+x_s<0$, 则

$$(\delta-x_3-\cdots-x_s)^2 \geqslant \delta^2 > s-1 \geqslant 2,$$

这是和 (4) 式相矛盾的. 所以 $x_3,\cdots,x_s$ 中至少有一个是正的. 假定其中还有一个是负的. 我们可以假定 $x_3 \geqslant 0, x_4<0$, 则

$$\begin{aligned}
&(\delta-(x_3+x_4)-x_5-\cdots-x_s)^2+2(x_3^2+\cdots+x_s^2)\\
\geqslant\ &(\delta-(x_3+x_4)-x_5-\cdots-x_s)^2+2((x_3+x_4)^2+x_5^2+\cdots+x_s^2)\\
\geqslant\ &\frac{2}{s-1}\delta^2>2
\end{aligned}$$

(由 1°). 这和 (4) 式相违背. 所以由 (4) 式可以自然地推出 (5) 及 (6). 故得

$$J(\delta)=\underset{(\delta-x_3-\cdots-x_s)^2<2(1-x_3^2-\cdots-x_s^2)}{\int\cdots\int}\frac{\mathrm{d}x_3\cdots\mathrm{d}x_s}{\sqrt{2(1-x_3^2-\cdots-x_s^2)-(\delta-x_3-\cdots-x_s)^2}}.$$

在 3° 中取 $n=s-2, A=2-\delta^2, L(x_1,\cdots,x_n)=\delta(x_3+\cdots+x_s)$ 及 $Q(x_3,\cdots,x_s)=(x_3+\cdots+x_s)^2+2(x_3^2+\cdots+x_s^2)$. 则由 4° 可知

$$|Q|=s\cdot 2^{s-3},\quad |\Delta|=2^{s-2}(s-\delta^2).$$

所以由 3° 得出

引理 10.12　若 $s \geqslant 3$ 及 $s \geqslant \delta^2 > s-1$, 则

$$J(\delta)=s^{1-\frac{1}{2}s}(s-\delta^2)^{\frac{1}{2}(s-3)}\frac{\pi^{\frac{1}{2}(s-1)}}{\Gamma\left(\frac{1}{2}(s-1)\right)}.$$

2) 同余可解条件的研究.

关于 $\mathfrak{S}(N_2, N_1)$ 的算出, 更为烦杂. 我们现在仅大概说明其计算方法, 并叙述其重要结论如次:

我们改写

$$T\left(\frac{u}{p^l}, \frac{v}{p^l}\right) = T(u, v, p^l). \quad (u, v) = 1.$$

用

$$S(u, p^l) = \sum_{x=1}^{p^l} e_{p^l}(ux^2)$$

代表普通的 Gauss 和. 关于此和的数值我们熟知有以下的结果:

1°

$$S(u, p^l) = \left(\frac{u}{p}\right)^l S(1, p^l), \quad 若 p > 2, \tag{7}$$

$$S(u, 2^l) = (-1)^{\frac{1}{8}(u^2-1)l} i^{-\frac{1}{4}(u-1)^2} S(1, 2^l), \tag{8}$$

$$S(1, p^l) = i^{\frac{1}{4}(p^l-1)^2} p^{\frac{1}{2}l}, \quad 若 p > 2, \tag{9}$$

$$S(1, 2^l) = \left\{ \begin{array}{ll} 0, & 若 l = 1, \\ (1+i)2^{\frac{1}{2}l}, & 若 l > 1. \end{array} \right\} \tag{10}$$

2° 我们引进整数 γ, 其定义是

$$p^\gamma \parallel (2u, v).$$

于是我们有以下的

引理 10.13　假定 $l > 2\gamma + 1$. 若同余式

$$2ux + v \equiv 0 \pmod{p^{\gamma+1}}, \quad p \nmid x \tag{11}$$

无解, 则

$$T(u, v, p^l) = 0. \tag{12}$$

若不然, 命 x_0 是

$$2ux + v \equiv 0 \pmod{p^{l+\gamma}} \tag{13}$$

的解, 则

$$T(u, v, p^l) = e_{p^l}(-ux_0^2) S(u, p^l) = e_{p^l}(-v^2/(4u)) S(u, p^l), \tag{14}$$

此处 $v^2/4u$ 和 $u\,x_0^2$ 是一对模 p^l 的整数.

证　命 $x=y+p^{l-\gamma-1}z$, 则

$$T(u,v,p^l)=\sum_{y,p^{l-\gamma-1}}{}^{*}e_{p^l}(uy^2+vy)\sum_{z,p^{\gamma+1}}e_{p^l}((2uy+v)p^{l-\gamma-1}z)$$
$$=p^{\gamma+1}\sum_{\substack{y,p^{l-\gamma-1}\\2uy+v\equiv 0(\bmod\ p^{\gamma+1})}}e_{p^l}(uy^2+vy),$$

此处 $\sum\limits_{y,p^l}$ 代表一和, y 经过一剩余系, mod p^l; $\sum\limits_{y,p^l}{}^{*}$ 代表一和, y 经过一既约剩余系, mod p^l.

显然当 (11) 无解时, 此和为零. 不然命 x_0 是适合 (13) 的解. 则 (11) 式所有的解可以表成

$$x=x_0+py,\quad 1\leqslant y\leqslant p^{l-1}.$$

以此代入原和, 即得

$$T(u,v,p^l)=\sum_{y,p^{l-1}}e_{p^l}(u(x_0+py)^2+v(x_0+py))$$
$$=e_{p^l}(ux_0^2+vx_0)\sum_{x,p^{l-1}}e_{p^{l-2}}(uy^2)$$
$$=e_{p^l}\left(-\frac{v^2}{4u}\right)pS(u,p^{l-2})$$
$$=e_{p^l}\left(-\frac{v^2}{4u}\right)S(u,p^l).$$

3° 当 $l\leqslant 2\gamma+1$ 时, $T(u,v,p^l)$ 可以一一算出; 特别是 $p>2$, 则 $\gamma=0$, 而有

$$T(u,v,p)=\sum_{x,p}e(ux^2+vx)-1$$
$$=\begin{cases}e_p\left(-\dfrac{v^2}{4u}\right)S(u,p)-1, & 若 p\nmid u,\\ -1, & 若 p|u.\end{cases}\tag{15}$$

当 $p=2$ 时, $l\leqslant 3$, 直接可以算出

$$\left.\begin{aligned}&T(u,v,2)=(-1)^{u+v},\\&T(u,v,4)=i^{u+v}(1+(-1)^v),\\&T(u,v,8)=\left(\frac{1+i}{\sqrt{2}}\right)^{u+v}(1+i^v)(1+(-1)^v).\end{aligned}\right\}\tag{16}$$

至此, 我们已经有了足够的方法来算出 $T(u,v,p^l)$ 的数值.

4° 命

$$A(p^l)=\sum_{\substack{u=1\\ p\nmid(u,v)}}^{p^l}\sum_{v=1}^{p^l}\left(\frac{T(u,v,p^l)}{\varphi(p^l)}\right)e_{p^l}(-N_2u-N_1v).$$

经冗长之计算后可以得出以下的二引理.

引理 10.14 　假定 $l>1$, 当 p^l 充分大时,

$$A(p^l)=0.$$

(在证明此引理时, 将用到 $sN_2-N_1^2\neq 0$, 而此点为正可解条件 $N_1^2<sN_2$ 所保证).

引理 10.15

$$A(p)\ll p^{1-\frac{1}{2}s}.$$

命

$$\partial_p=\sum_{l=0}^{\infty}A(p^l).$$

由引理 10.14 可知 ∂_p 仅是一个有限的级数. 并且当 p 充分大时,

$$\partial_p=1+A(p).$$

再由引理 10.15 可知: 当 $s\geqslant 5$ 时,

$$\prod_p\partial_p$$

是一绝对收敛的无穷乘积. 由此可知

引理 10.16 　当 $s\geqslant 5$ 时,

$$\mathfrak{S}(N_2,N_1)=\prod_p\partial_p$$

是一绝对收敛的级数.

5° 更复杂的计算可以证明:

当 $s\geqslant 5$ 及 $p\geqslant 5$ 时, $\partial_p>0$; 又若 $2|(s-N_1)$ 及 $8|(s-N_2)$ 时, $\partial_2>0$; 而若 $3|(s-N_2)$ 时, $\partial_3>0$. 总之, 可以证明

引理 10.17 　命 $s\geqslant 5$. 若 $2|(s-N_1)$ 及 $24|(s-N_2)$, 则

$$\mathfrak{S}(N_2,N_1)>0.$$

把本节的结果和定理 17 联合起来, 可以得出以下的更明确的结论:

命 $N_1(t), N_2(t)$ 是两组正整数随 t 趋向无穷. 假定

$$l < \varlimsup_{t\to\infty} \frac{N_1^2(t)}{N_2(t)} < 7.$$

并假定 $N_1(t)$ 是奇数, $N_2(t) \equiv 7(\mathrm{mod}24)$, 则当 t 充分大时, 有七个素数 $p_1, \cdots, p_7$ 使

$$p^2 + \cdots + p_7^2 = N_2,$$
$$p_1 + \cdots + p_7 = N_1.$$

第 11 章　前章问题进一步的研究

§11.1

本章中将阐明"正可解条件"及"同余可解条件"的含义并将给与一些条件来保证"正可解"及"同余可解". 因之, 在这些条件之下, 及当 $s > 2k^2(3\log k + \log\log k + 4)$ 及 N 充分大时, 方程组

$$\begin{aligned} p_1^k + \cdots + p_s^k &= N_k, \\ &\cdots\cdots \\ p_1 + \cdots + p_s &= N_1 \end{aligned} \tag{1}$$

有素数解.

本章的另一目的在缩小 s 的限制. 换言之, 我们将把 s 所大于的数减低成为

$$2k^2 + 3 + k\log(50k^3\log k) \,/\, \log\frac{1}{1-a} \sim 3k^2\log k,$$

即当 s 大于上数及充分大的 $N_k, \cdots, N_1$ 适合"正可解"及"同余可解"的条件时, 上方程组有解答.

§11.2　正可解条件的研究

命

$$b_1 = \int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x)\mathrm{d}x\right)^s e(-\gamma_k\delta_k - \gamma_{k-1}\delta_{k-1} - \cdots - \gamma_1\delta_1)\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1.$$

命

$$B(w_k, \cdots, w_1) = \int_{-w_k}^{w_k}\mathrm{d}\gamma_k\cdots\int_{-w_1}^{w_1}\left(\int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x)\mathrm{d}x\right)^s e(-\gamma_k\delta_k - \gamma_{k-1}\delta_{k-1} - \cdots - \gamma_1\delta_1)\mathrm{d}\gamma_1.$$

如是, 由定义

$$b_1 = \lim_{w_k\to\infty}\cdots\lim_{w_1\to\infty} B(\omega_k, \cdots, \omega_1).$$

交换积分号, 可得

$$B(\omega)=B(\omega_k,\cdots,\omega_1)=\int_0^1\cdots\int_0^1 \mathrm{d}x_1\cdots\mathrm{d}x_s$$
$$\times\int_{-\omega_k}^{\omega_k}\cdots\int_{-\omega_1}^{\omega_1} e(\gamma_k(x_1^k+\cdots+x_s^k-\delta_k)+\cdots+\gamma_1(x_1+\cdots+x_s-\delta_1))\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1$$
$$=\int_0^1\cdots\int_0^1 \frac{\sin 2\pi\omega_k(x_1^k+\cdots+x_s^k-\delta_k)}{\pi(x_1^k+\cdots+x_s^k-\delta_k)}\cdots\frac{\sin 2\pi\omega_1(x_1+\cdots+x_s-\delta_1)}{\pi(x_1+\cdots+x_s-\delta_1)}\mathrm{d}x_1\cdots\mathrm{d}x_s.$$

命

$$\left.\begin{aligned} X_1&=x_1+\cdots+x_s-\delta_1,\\ &\cdots\cdots\\ X_k&=x_1^k+\cdots+x_s^k-\delta_k,\end{aligned}\right\}$$

则函数行列式

$$J=\frac{D(x_1,\cdots,x_k)}{D(X_1,\cdots,X_k)}=\frac{1}{k!}\begin{vmatrix}1&\cdots&1\\ x_1&\cdots&x_k\\ \vdots&&\vdots\\ x_1^{k-1}&\cdots&x_k^{k-1}\end{vmatrix}^{-1}=\frac{1}{k!\prod\limits_{k\geqslant i>j\geqslant 1}(x_i-x_j)}.$$

把 k 维单位方体分成若干份 D_j, 在每一份中 J 都不变号. 如此则得

$$B(w)=\sum_j\int\underset{D_j}{\cdots}\int\frac{\sin 2\pi w_1X_1}{\pi X_1}\cdots\frac{\sin 2\pi w_kX_k}{\pi X_k}\mathrm{d}X_1\cdots\mathrm{d}X_k$$
$$\times\underset{\substack{0\leqslant x_1\leqslant 1\\ \cdots\\ 0\leqslant x_k\leqslant 1}}{\int_0^1\cdots\int_0^1}\frac{\mathrm{d}x_{k+1}\cdots\mathrm{d}x_s}{k!\Pi(x_i-x_j)}.$$

由 Dirichlet 定理可知: 如果方程组

$$X_\mu=x_1^\mu+\cdots+x_s^\mu-\delta_\mu=0,\quad x_v\leqslant 1,\ 1\leqslant\mu\leqslant k, \tag{2}$$

有正数解答, 则

$$\lim_{\omega\to\infty}B(\omega)=\underset{\substack{0\leqslant x_\nu\leqslant 1\\ X_\nu=0}}{\int_0^1\cdots\int_0^1}\frac{\mathrm{d}x_{k+1}\cdots\mathrm{d}x_s}{k!|\Pi(x_i-x_j)|}>0. \tag{3}$$

所以我们一变而为求

$$x_1^\mu+\cdots+x_s^\mu=\delta_\mu,\quad 0\leqslant x_\nu\leqslant 1,\ 1\leqslant\mu\leqslant k,\ 1\leqslant\nu\leqslant s,$$

有正数解答的问题. 用 $\delta_\mu = N_\mu/P^\mu$ 代入, 也就是

$$Z_1^\mu + \cdots + Z_s^\mu = N_\mu, \quad 1 \leqslant \mu \leqslant k, \tag{4}$$

有无正数解答的问题. 这一条件十分自然, 因为如果连正数的解答都没有, 还谈什么有正整数解的问题, 更勿论有素数解的问题. 尚须注意者, 因为 $N_k^a = P$, 所以 $\delta_k = 1$, 因之 $x_\nu \leqslant 1$ 也是自然的结果, 而不必另添假定了.

所以 "正可解条件" 就是保证 (4) 式有正数解答的条件, 这是命名的由来.

引理 11.1 方程组

$$x_1^h + \cdots + x_k^h = \delta_h, \quad 1 \leqslant h \leqslant k \tag{5}$$

有正数解, 且 $x_i \neq x_j (i \neq j)$, 的必要且充分条件是二次型

$$\sum_{i,j=1}^{k} \delta_{i+j-1} t_i t_j \tag{6}$$

是定正的, 此处 $\delta_\nu (\nu > k)$ 可由次式巡回定义之:

$$\begin{vmatrix} \delta_1, & 1, & 0, & \cdots, & 0 \\ \delta_2, & \delta_1, & 2, & \cdots, & 0 \\ & \vdots & & \vdots & \\ \delta_k, & \delta_{k-1}, & \delta_{k-2}, & \cdots, & k \\ \delta_\nu, & \delta_{\nu-1}, & \delta_{\nu-2}, & \cdots, & \delta_{\nu-k} \end{vmatrix} = 0.$$

证 1) 必要性. 如 (1) 式有解, 命

$$R_\nu = t_1 x_\nu + t_2 x_\nu^2 + \cdots + t_k x_\nu^k,$$

则

$$\sum_{\nu=1}^{k} \frac{1}{x_\nu} R_\nu^2 = \sum_{i,j=1}^{k} \delta_{i+j-1} t_i t_j$$

显然是一定正二次型.

2) 充分性. (5) 式一定有解的, 虽然我们并不能断定它是复数抑是实数. 把 $x_1, \cdots, x_k$ 作根作一多项式, 如此作出的 k 次多项式是有实系数的. 所以, 如果 $x_1, \cdots, x_k$ 中有复数出现, 一定是一对对的共轭复数. $x_1, \cdots, x_k$ 各不相同, 且无一是零. 如若不然, $R_\nu = 0 (1 \leqslant \nu \leqslant k)$ 有一非零解 $(t_1, \cdots, t_k)$, (零解我们是指 $t_1 = 0, \cdots, t_k = 0$ 这一解). 因而 (6) 非定正型. 把根 $x_1, \cdots, x_k$ 排成

$$\begin{aligned} x_{2m-1} &= y_{2m-1} + i y_{2m}, \\ x_{2m} &= y_{2m-1} - i y_{2m}, \end{aligned} \qquad y_{2m} \neq 0, \quad 1 \leqslant m \leqslant g$$

及

$$x'_\nu = y_\nu, \quad 2g < \nu \leqslant k,$$

此处 y 是实数. 为

$$\begin{aligned} R_{2m-1}/x_{2m-1} &= P_{2m-1} + iP_{2m}, \\ R_{2m}/x_{2m} &= P_{2m-1} - iP_{2m}, \end{aligned} \quad 1 \leqslant m \leqslant g.$$

此处 $P_v (1 \leqslant v \leqslant 2g)$ 是 $t_1, \cdots, t_k$ 的实系数线性式. 解方程组

$$\begin{aligned} P_v &= 0, \quad 3 \leqslant v \leqslant 2g, \\ R_v &= 0, \quad 2g < v \leqslant k \end{aligned}$$

及

$$y_1 P_1 = \left(y_2 + \sqrt{y_1^2 + y_2^2} \right) P_2.$$

这是 $k-1$ 个实系数的线性方程组, 有 k 个变数 $t_1, \cdots, t_k$. 显然有一不同于零解的解答 $t_1, \cdots, t_k$. 对这一解, 我们有

$$\begin{aligned} \sum_{v=1}^{k} \frac{1}{x_v} R_v^2 = \sum_{v=1}^{k} x_v \left(\frac{R_v}{x_v} \right)^2 &= x_1 \left(\frac{R_1}{x_1} \right)^2 + x_2 \left(\frac{R_2}{x_2} \right)^2 \\ &= 2y_1 (P_1^2 - P_2^2) - 4y_2 P_1 P_2 = 0. \end{aligned}$$

这和 (6) 是定正型的假设相违背. 所以 $x_1, \cdots, x_k$ 都是实数. 由

$$\sum_{v=1}^{k} \frac{1}{x_v} R_v^2$$

的形式, 立刻可以看出: 如果上式是定正型, 则 x_v 都是正数.

附记: 由于连续性, 引理 11.1 可以作如下的修改而仍然真实: 一方面取消条件 $x_i \neq x_j$, 另一方面把定正性改为半定正性. 更推广些, 有

引理 11.2　命 $s \geqslant k$. 方程组

$$x_1^h + \cdots + x_s^h = \delta_h, \quad 1 \leqslant h \leqslant k$$

有正实数解的必要且充分条件是: 有 $s-k$ 个正数 $\delta_{k+1}, \cdots, \delta_s$ 存在使

$$\sum_{i,j=1}^{s} \delta_{i+j-1} t_i t_j$$

是一半定正型, 而 $\delta_v(v>s)$ 是由次之关系巡回地定义出来的:

$$\begin{vmatrix} \delta_1, & 1, & 0, & \cdots, & 0 \\ \delta_2, & \delta_1, & 2, & \cdots, & 0 \\ & \vdots & & \vdots & \\ \delta_k, & \delta_{k-1}, & \delta_{k-2}, & \cdots, & k \\ \delta_v, & \delta_{v-1}, & \delta_{v-2}, & \cdots, & \delta_{v-k} \end{vmatrix} = 0.$$

因为和引理 11.1 的证明相同, 所以略去不证.

附记: 如果仅需实数解, 而不限定是正数解, 则

$$\sum_{i,j=1}^{n} \delta_{i+j-2} t_i t_j, \quad \delta_0 = s,$$

的半定正性就可以保证.

引理 11.3 如有 $k-1$ 个正数 $\delta_1, \cdots, \delta_{k-1}$ 及 $\delta_k = 1$ 适合引理 11.2 的条件, 命 $N_v = [\delta_v P^v]$, 则对这一组 $N_1, \cdots, N_k$ 正可解条件有了保证.

这引理的证明十分显然. 当然我们还可以把加于 δ 的条件改变成为加于 N 的条件.

§11.3 奇异级数与同余可解条件

今用 $\sum\limits_{x,(q)}$ 代表一和, 其中的变数 x 经过一完整剩余系, mod q. 又用 $\sum\limits_{x,(q)}{}'$ 代表一和, 其中的变数 x 经过一既约剩余系, mod q. 已有.

$$\mathfrak{S} = \mathfrak{S}(N_k, \cdots, N_1) = \sum_{q_1=1}^{\infty} \cdots \sum_{q_k=1}^{\infty} A(q_k, \cdots, q_1),$$

$$A(q_k, \cdots, q_1) = \sum_{h_1,(q_1)}{}' \cdots \sum_{h_k,(q_k)}{}' T^s e\left(-\frac{h_k}{q_k} N_k - \cdots - \frac{h_1}{q_1} N_1\right),$$

$$T = \frac{1}{\varphi(Q)} T\left(\frac{h_k}{q_k}, \cdots, \frac{h_1}{q_1}\right) = \frac{1}{\varphi(Q)} \sum_{x,(Q)}{}' e\left(\frac{h_k}{q_k} x^k + \cdots + \frac{h_1}{q_1} x\right),$$

此处 Q 为 $q_1, \cdots, q_k$ 的最小公倍数.

引理 11.4 $\mathfrak{S}$ 亦可以改写成

$$\mathfrak{S} = \sum_{Q=1}^{\infty} \sum_{\substack{a_k=1 \\ (a_k,\cdots,a_1,Q)=1}}^{Q} \cdots \sum_{a_1=1}^{Q} \left(\frac{1}{\varphi(Q)} \sum_{x,(Q)}{}' e_Q(a_k x^k + \cdots + a_1 x)\right)^s e_Q(-a_k N_k - \cdots - a_1 N_1).$$

证　这一引理是以下事实的直接推理：从关系

$$h_lQ/q_l = a_l, \quad l = 1, 2, \cdots, k,$$

可知以下二数列是一一对应的：(i) $\mathfrak{S}$ 的原定义中所展过的数列

$$q_l = 1, 2, 3, \cdots, (h_l, q_l) = 1, \quad 1 \leqslant h_l \leqslant q_l, \quad l = 1, 2, \cdots, k$$

及 (ii) 引理中所展过的数列

$$Q = 1, 2, 3, \cdots, (a_k, \cdots, a_1, Q) = 1, 1 \leqslant a_l \leqslant Q, l = 1, 2, \cdots, k.$$

这一事实几乎显然，所以不加证明.

命 $W(m)$ 代表同余式组

$$\left.\begin{array}{c} h_1^k + \cdots + h_s^k \equiv N_k, \\ \cdots\cdots \\ h_1 + \cdots + h_s \equiv N_1. \end{array}\right\} \pmod{m}, \tag{1}$$

$$1 \leqslant h_v \leqslant m, \quad (h_v, m) = 1, \quad 1 \leqslant v \leqslant s$$

的解数. 显然可证

引理 11.5　若 $(m_1, m_2) = 1$，则

$$W(m_1, m_2) = W(m_1)W(m_2).$$

定义

$$A(Q) = \sum_{\substack{a_k=1 \\ (a_k,\cdots,a_1,Q)=1}}^{Q} \cdots \sum_{a_1=1}^{Q} \left(\frac{1}{\varphi(Q)} T\left(\frac{a_k}{Q}, \cdots, \frac{a_1}{Q}\right)\right)^s e_Q(-a_kN_k - \cdots - a_1N_1)$$

及

$$\partial_p = \sum_{l=0}^{\infty} A(p^l), \quad A(1) = 1.$$

引理 11.6

$$\sum_{m=0}^{l} A(p^m) = p^{lk}\varphi^{-s}(p^l)W(p^l).$$

证　显然

$$W(p^l) = \frac{1}{p^{lk}} \sum_{h_1=1}^{p^l} \cdots \sum_{h_k=1}^{p^l} \sum_{x_1=1}^{p^l}{}' \cdots \sum_{x_s=1}^{p^l}{}'$$

$$
\begin{aligned}
&e_p^l\left(h_k(x_1^k+\cdots+x_s^k-N_k)+\cdots+h_1(x_1+\cdots+x_s-N_1)\right)\\
&=\frac{1}{p^{lk}}\varphi^s(p^l)\sum_{h_1=1}^{p^l}\cdots\sum_{h_k=1}^{p^l}\left(\frac{1}{\varphi(p^l)}T\left(\frac{h_k}{p^l},\cdots,\frac{h_1}{p^l}\right)\right)^s e_{p^l}(-h_kN_k-\cdots-h_1N_1)\\
&=\frac{1}{p^{lk}}\varphi^s(p^l)\Bigg(\sum_{\substack{h_1=1\\ p|h_1}}^{p^l}\cdots\sum_{\substack{h_k=1\\ p|h_k}}^{p^l}\left(\frac{1}{\varphi(p^l)}T\left(\frac{h_k}{p^l},\cdots,\frac{h_1}{p^l}\right)\right)^s e_{p^l}(-h_kN_k-\cdots-h_1N_1)\\
&\quad+A(p^l)\Bigg)\\
&=\frac{1}{p^{lk}}\varphi^s(p^l)\Bigg(\sum_{h_1=1}^{p^{l-1}}\cdots\sum_{h_k=1}^{p^{l-1}}\left(\frac{1}{\varphi(p^{l-1})}T\left(\frac{h_k}{p^{l-1}},\cdots,\frac{h_1}{p^{l-1}}\right)\right)^s e_{p^{l-1}}(-h_kN_k\\
&\quad-\cdots-h_1N_1)+A(p^l)\Bigg).
\end{aligned}
$$

续行此法可得本引理.

引理 11.7 当 $s>k^2$ 时, ∂_p 收敛; 且当 $s>k^2+k$ 时, 有

$$|\partial_p-1|\leqslant 2(2k^3)^sp^{k-as}$$

及

$$\mathfrak{S}=\prod_p\partial_p.$$

证 由第一章基本引理已知

$$\left|T\left(\frac{h_k}{p^l},\cdots,\frac{h_1}{p^l}\right)\right|\leqslant k^3p^{l(1-a)}.$$

由此可知,

$$|A(p^l)|\leqslant(p^{lk}-p^{(l-1)k})\left(\frac{k^3p^{l(1-a)}}{p^{l-1}(p-1)}\right)^s<(2k^3)^sp^{l(k-as)}.$$

所以当 $s>k^2$ 时, ∂_p 绝对收敛. 又当 $s>k^2+k$ 时,

$$|\partial_p-1|\leqslant(2k^3)^s\sum_{l=1}^{\infty}p^{l(k-as)}\leqslant(2k^3)^s\frac{p^{k-as}}{1-p^{k-as}}\leqslant 2(2k^3)^sp^{k-as}.$$

最后一个结论可由

$$\sum_p p^{k-as}$$

的收敛性得之.

说明　由引理 11.6 及 11.7, 可知

$$\partial_p = \lim_{l\to\infty} p^{lk}\varphi^{-s}(p^l)W(p^l).$$

容易看出, 如果有一 l_0 使 $W(p^{l_0})=0$, 则显然对 $l>l_0, W(p^l)$ 也等于 0. 所以 $\partial_p=0$ 及 $\mathfrak{S}=0$. 具体地说: 如果同余式 (1) 不可解, 则我们所讨论的问题就无解答. 这是一个十分自然的现象, 也是同余可解条件命名的理由. 引理 11.7 还告诉了我们另一事实:

引理 11.8　当 $p>(2(2k^3)^s)^{\frac{1}{as-k}}$ 时,

$$\partial_p>0,$$

即同余式 (1) 当 $m=p^l$ 时常可解.

命

$$D=\begin{vmatrix} k^{k-1}, & \cdots, & 2^{k-1}, & 1^{k-1} \\ & \cdots\cdots & & \\ k, & \cdots, & 2, & 1 \\ 1, & \cdots, & 1, & 1 \end{vmatrix}=(k-1)!(k-2)!\cdots 2!1!$$

及 $p^{\Theta}\parallel D$. 则当 $p>k$ 时 $\Theta=0$. 命

$$p^{\Theta_v}\parallel v,\quad v=p^{\Theta_v}v_0,\quad \Theta_0=\max(\Theta_1,\cdots,\Theta_k).$$

命 $W_1(p^l)$ 代表下列同余式组的解数;

$$\left.\begin{array}{c} y_1^k+\cdots+y_s^k\equiv N_k, \\ \cdots\cdots \\ y_1+\cdots+y_s\equiv N_1, \end{array}\right\}\quad (\bmod p^l), p\times y.$$

其中

$$1\leqslant y_v\leqslant p^l,\quad 1\leqslant v\leqslant k,\quad 1\leqslant y_\mu\leqslant p^{l-\Theta-\Theta_0},\quad k+1\leqslant \mu\leqslant s$$

及

$$p^{\Theta}\parallel\begin{vmatrix} y_k^{k-1}, & \cdots, & y_1^{k-1}, \\ & \cdots\cdots\cdots\cdots\cdots & \\ y_k, & \cdots, & y_1 \\ 1, & \cdots, & 1 \end{vmatrix}.$$

引理 11.9　同余式组

$$\sum_{\beta=1}^{k} a_{\alpha\beta}x_\beta\equiv b_\alpha\quad (\bmod p^l),\quad 1\leqslant\alpha\leqslant k,$$

$$p^{\lambda} \| \begin{vmatrix} a_{11}, & \cdots, & a_{1k} \\ \cdots & \cdots & \cdots \\ a_{k1}, & \cdots, & a_{kk} \end{vmatrix},$$

可解的条件是:

$$p^{\lambda} \left| \begin{vmatrix} b_1, & a_{12}, & \cdots, & a_{1k} \\ \cdots & \cdots & \cdots & \cdots \\ b_k, & a_{k2}, & \cdots, & a_{kk} \end{vmatrix}, \quad \cdots, \quad p^{\lambda} \right| \begin{vmatrix} a_{11}, & \cdots, & a_{1,k-1}, & b_1 \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1}, & \cdots, & a_{k,k-1}, & b_k \end{vmatrix}.$$

证　这引理可用通常的行列式方法证明.

引理 11.10　当 $l \geqslant 2\Theta + 2\Theta_0 + 1$, 则

$$W_1(p^{l+1}) \geqslant p^{s-k} W_1(p^l).$$

连续运用多次可得

$$W_1(p^{l+u}) \geqslant p^{u(s-k)} W_1(p^l).$$

证　假定我们已经有了

$$\sum_{\mu=1}^{s} y_\mu^v \equiv N_v \pmod{p^l}, \tag{2}$$

$$1 \leqslant y_\lambda \leqslant p^l, \quad 1 \leqslant \lambda \leqslant k; \quad 1 \leqslant y_\tau \leqslant p^{l-\Theta-\Theta_0}, \quad k+1 \leqslant \tau \leqslant s.$$

命

$$h_\mu = y_\mu + z_\mu p^{l-\Theta_0-\Theta},$$

则

$$h_\mu^v \equiv y_\mu^v + v y_\mu^{v-1} z_\mu p^{l-\Theta_0-\Theta} \pmod{p^{2(l-\Theta_0-\Theta)}},$$

$$\sum_{\mu=1}^{s} h_\mu^v \equiv \sum_{\mu=1}^{s} y_\mu^v + v \sum_{\mu=1}^{s} y_\mu^{v-1} z_\mu p^{l-\Theta_0-\Theta} \pmod{p^{l+1}}. \tag{3}$$

今讨论同余式组

$$\sum_{\mu=1}^{s} v_0 y_\mu^{v-1} z_\mu \equiv \frac{N_v - \sum\limits_{\mu=1}^{s} y_\mu^v}{p^{l-\Theta_0-\Theta+\Theta_v}} \pmod{p^{\Theta_0+\Theta+1}}. \tag{4}$$

如果 (4) 有解, 则由 (3)

$$\sum_{\mu=1}^{s} h_\mu^v \equiv N_v \pmod{p^{l+1}}. \tag{5}$$

由于

$$p^{\Theta} \parallel \begin{vmatrix} y_1^{k-1}, & \cdots, & y_k^{k-1} \\ \cdots & \cdots & \cdots \\ y_1^0, & \cdots, & y_k^0 \end{vmatrix}$$

及

$$p^{\Theta} | p^{\Theta_0+\Theta-\Theta_v} | \frac{N_v - \sum_{\mu=1}^{s} y_\mu^v}{p^{l-\Theta_0-\Theta+\Theta_v}},$$

所以对任意的 $z_\tau(k+1 \leqslant \tau \leqslant s)$, 同余式组 (4) 式常可解. 所以

$$W_1(p^{l+1}) \geqslant p^{s-k} W_1(p^l).$$

证明中如无以下的补充, 还不能算是完整的：由于 $h_\mu \equiv y_\mu (\text{mod} p^{l-\Theta_0-\Theta})$, 所以

$$\begin{vmatrix} y_1^{k-1}, & \cdots, & y_k^{k-1} \\ \cdots & \cdots & \cdots \\ y_1^0, & \cdots, & y_k^0 \end{vmatrix} \equiv \begin{vmatrix} h_1^{k-1}, & \cdots, & h_k^{k-1} \\ \cdots & \cdots & \cdots \\ h_1^0, & \cdots, & h_k^0 \end{vmatrix} \quad (\text{mod} p^{\Theta+1}),$$

此处用了 $l > \Theta_0 + 2\Theta$.

引理 11.11　设 $s > k^2 + k$, 并设当 $p \leqslant (2(2k^3)^s)^{\frac{1}{as-k}}$ 时,

$$W_1(p^{2\Theta+2\Theta_0}) > 0.$$

则 $\mathfrak{S}(N_k, \cdots, N_1)$ 大于一并不依赖于 N 的常数.

证　由假定及引理 11.10 已知, 当 $p \leqslant (2(2k^3)^s)^{\frac{1}{as-k}}$ 时,

$$\begin{aligned} \partial_p &= \lim_{l\to\infty} p^{lk} \varphi^{-s}(p^l) W(p^l) \\ &\geqslant \lim_{l\to\infty} p^{lk} \varphi^{-s}(p^l) W_1(p^l) \\ &\geqslant \lim_{l\to\infty} p^{lk} \varphi^{-s}(p^l) p^{(s-k)(l-2\Theta-2\Theta_0)} W_1(p^{2\Theta+2\Theta_0}) \\ &\geqslant \lim_{l\to\infty} \frac{p^{-l(s-k)}}{(1-1/p)^s} p^{(s-k)(l-2\Theta-2\Theta_0)} \\ &= p^{-(s-k)(2\Theta-2\Theta_0)} \left(1 - \frac{1}{p}\right)^{-s} \geqslant c_1, \end{aligned}$$

这 c_1(及今后 c_2, c_3) 与 N 无关, 且 > 0.

命 $s = k^2 + k + \delta$, 则

$$\partial_p > 1 - 2(2k^3)^s p^{-1-\delta a}.$$

当 p 适合 $(2(2k^3)^s)^{\frac{1}{as-k}} < p \leqslant (2(2k^3)^s)^{2k/\delta}$, 显然 $\partial_p \geqslant c_2$.

又当 $p > (2(2k^3)^s)^{2k/\delta}$, 则

$$\partial_p > 1 - p^{-1-\frac{1}{2}\delta a}.$$

所以

$$\prod_{p>(2(2k^3)^s)^{2k/\delta}} \partial_p \geqslant c_3.$$

总之, 可知

$$\mathfrak{S}(N_k, \cdots, N_1) \geqslant (c_1 c_2)(2(2k^3)^s)^{2k/\delta} c_3.$$

引理已经证明.

今再进一步讨论

$$W_1(p^{2\Theta+2\Theta_0}) \geqslant 1$$

的条件.

引理 11.12 若 $p > k$ 及 $s > (k+1)p$, 则 $W_1(p) \geqslant 1$.

证 同余式组

$$x_1(k+1)^v + x_2 k^v + x_3(k-1)^v + \cdots + x_{k+1}1^v \equiv N_v (\bmod p), \quad 1 \leqslant v \leqslant k,$$
$$x_1 + x_2 + x_3 + \cdots + x_{k+1} \equiv s (\bmod p)$$

常有解在 $0 < x_v \leqslant p$ 中. 故可取 x_{k+1} 使

$$x_1 + \cdots + x_{k+1} = s.$$

所以得出本引理.

引理 11.13 当 $s > 2k$ 及 $p > k^{k(s-k)/(s-2k)}$ 时, 同余式组

$$x_1^v + \cdots + x_s^v \equiv N_v \quad (\bmod p), p \times x, 1 \leqslant v \leqslant k$$

有解.

证 这同余式的解的组数 M 显然等于

$$\frac{1}{p^k} \sum_{a_1=1}^{p} \cdots \sum_{a_k=1}^{p} \left(\sum_{x=1}^{p-1} e_p(a_k x^k + \cdots + a_1 x) \right)^s e_p(-(a_k N_k + \cdots + a_1 N_1)).$$

故

$$|M - p^{s-k}| \leqslant \frac{1}{p^k} \sum_{a_1=1}^{p} \cdots \sum_{a_k=1}^{p}{}^{*} \left| \sum_{x=1}^{p-1} e_p(a_k x^k + \cdots + a_1 x) \right|^s,$$

此处 $*$ 乃表示 p 不能同时整除所有的 a. 由第一章 §3 公式 (2) 及 (3) 得出

$$\begin{aligned}|M-p^{s-k}| &\leqslant \frac{1}{p^k}(kp^{1-a})^{s-2k}\sum_{a_1=1}^{p}\cdots\sum_{a_k=1}^{p}\left|\sum_{x=1}^{p-1}e_p(a_kx^k+\cdots+a_1x)\right|^{2k}\\ &\leqslant \frac{1}{p^k}(kp^{1-a})^{s-2k}k!p^{2k}\\ &\leqslant k^{s-k}p^{s-k-a(s-2k)}\\ &< p^{s-k},\end{aligned}$$

此处用了条件 $p>k^{k(s-k)/(s-2k)}$. 因此得出

$$M\geqslant p^{s-1}-(p^{s-1}-1)=1.$$

此即本引理.

引理 11.14　当 $s>3k$ 及 $p>k^{k(s-k)/(s-2k)}$ 时, 则

$$W_1(p)\geqslant 1.$$

证　由引理 11.13, 当 $t>2k,p>k^{k(s-k)/(s-2k)}$ 时, 同余式组

$$x_1^v+\cdots+x_t^v\equiv N_v-1^v-2^v-\cdots-k^v \pmod p \quad p\nmid x, 1\leqslant v\leqslant k,$$

常有解. 由此得出本引理.

附记: 本节所说的结果十分粗略, 大有更进一步的可能.

§11.4

引理 11.15　命

$$(2v-1)Q\leqslant x_v\leqslant 2vQ,\quad 1\leqslant v\leqslant k.$$

则整数组 $x_1,\cdots,x_k$ 中, 使

$$x_1^h+\cdots+x_k^h,\quad 1\leqslant h\leqslant k,$$

各落在长 $\ll Q^{h-1}(1\leqslant h\leqslant k)$ 隔间中的组数 $\ll 1$.

这引理的证明如同引理 4.1 的证明一样, 不要经过任何本质上的改变.

引理 11.16　命 R_k 表方程组

$$\sum_{j=1}^{n}\sum_{i=1}^{k}x_{ij}^h=\sum_{j=1}^{n}\sum_{i=1}^{k}x_{ij}'^h,\quad 1\leqslant h\leqslant k, \tag{1}$$

$$(2i-1)P^{(1-a)^{i-1}} \leqslant x_{ij}, x'_{ij} \leqslant 2iP^{(1-a)^{j-1}} \tag{2}$$

的整数解的组数. 则

$$R_k \leqslant P^{(2k^2-\frac{1}{2}k(k+1))(1-(1-a)^n)}.$$

证　由 (1) 及 (2) 易见

$$\sum_{i=1}^{k} x_{i1}^h - \sum_{i=1}^{k} x_{i1}'^h \ll P^{h(1-a)}, \quad 1 \leqslant h \leqslant k.$$

对已定的 $x'_{i1}(i=1,\cdots,k)$,

$$\sum_{i=1}^{k} x_{i1}^k, \sum_{i=1}^{k} x_{i1}^{k-1}, \cdots, \sum_{i=1}^{k} x_{i1}$$

各在长是

$$O(P^{k(1-a)}), \quad O(P^{(k-1)(1-a)}), \quad \cdots, O(P^{(1-a)}) \tag{3}$$

的隔间中. 把 (3) 的隔间组分为

$$O\left(\frac{P^{k(1-a)}}{P^{k-1}} \frac{P^{(k-1)(1-a)}}{P^{k-2}} \cdots \frac{P^{2(1-a)}}{P} \frac{P^{1-a}}{1}\right) = O(P^{k-\frac{1}{2}(k+1)})$$

个组, 而每一组是由长为

$$O(P^{k-1}), \quad O(P^{k-2}), \quad \cdots, \quad O(P), \quad O(1)$$

的隔间所组成的. 由引理 11.15(取 $Q=P$), 可知 $x_{i1}(1 \leqslant i \leqslant k)$ 的组数 $\ll P^{k-\frac{1}{2}(k+1)}$. 因此 x_{i1} 及 $x'_{i1}(i=1,\cdots,k)$ 的组数是

$$\ll P^{2k-\frac{1}{2}(k+1)}.$$

又, 对已定的 $x_{ij}, x'_{ij}(1 \leqslant i \leqslant k, 1 \leqslant j \leqslant l-1)$ 及 $x'_{il}(1 \leqslant i \leqslant k)$, 由 (1) 及 (2) 可知

$$\sum_{i=1}^{k} x_{il}^k, \quad \sum_{i=1}^{k} x_{il}^{k-1}, \quad \cdots, \quad \sum_{i=1}^{k} x_{il}$$

各落在长是

$$O(P^{k(1-a)^l}), \quad O(P^{k-1(1-a)^l}), \quad \cdots, \quad O(P^{(1-a)^l})$$

的隔间中. 由于

$$O\left(\frac{P^{k(1-a)^l}}{P^{(k-1)(1-a)^{l-1}}} \frac{P^{(k-1)(1-a)^l}}{P^{(k-2)(1-a)^{l-1}}} \cdots \frac{P^{(1-a)^l}}{1}\right) = O(P^{(k-\frac{1}{2}(k+1))(1-a)^{l-1}})$$

及由引理 11.15(取 $Q=P^{(I-a)^{l-1}}$) 可知 $x_{il}(1\leqslant i\leqslant k)$ 的组数是

$$O(P^{(k-\frac{1}{2}(k+1))(1-a)^{l-1}}).$$

因此, 对已定的 $x_{ij},x'_{ij}(1\leqslant i\leqslant k,1\leqslant j\leqslant l-1),x_{il}$ 及 x'_{il} 的组数是

$$O(P^{(2k-\frac{1}{2}(k+1))(1-a)^{l-1}}).$$

所以 (1) 式受 (2) 式限制的解数

$$\begin{aligned}&\ll P^{(2k-\frac{1}{2}(k+1))(1+(1-a)+\cdots+(1-a)^{n-1})}\\&=P^{(2k^2-\frac{1}{2}k(k+1))(1-(1-a)^n)}.\end{aligned}$$

§11.5

命

$$S_0=\sum_{n\leqslant 2kP}e(\alpha_kn^k+\cdots+\alpha_1n),$$

$$S_{ij}(\alpha_k,\cdots,\alpha_1)=\sum_{(2i-1)P^{(1-a)^{(j-1)}}\leqslant n\leqslant 2iP^{(1-a)^{(j-1)}}}e(\alpha_kn^k+\cdots+\alpha_1n),$$

此处 $1\leqslant i\leqslant k,1\leqslant j\leqslant n$.

引理 11.17 命 $t=k^2+1$ 及

$$n=\left[\frac{\log(50k^3\log k)}{-\log(1-a)}\right]+1,$$

则

$$\int_0^1\cdots\int_0^1|S_0|^{2t}\prod_{j=1}^n\prod_{i=1}^k|S_{ij}|^2\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1\ll P^{2t+2k^2(1-(1-a)^n)-\frac{1}{2}k(k+1)}.$$

证 如定理 15 证明中的方法来分割积分的范围. 由于 $t\geqslant k^2+1$, 所以

$$\sum_{\mathfrak{M}}\int\underset{\mathfrak{M}}{\cdots}\int|S_0|^{2t}\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1\ll P^{2t-\frac{1}{2}k(k+1)}$$

(一如定理 15 中之所写). 因此

$$\sum_{\mathfrak{M}}\int\underset{\mathfrak{M}}{\cdots}\int|S_0|^{2t}\left|\prod_{j=1}^n\prod_{i=1}^kS_{ij}\right|^2\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1$$

$$\ll \max_{a}\left|\prod_{j=1}^{n}\prod_{i=1}^{k}S_{ij}\right|^2 \times \sum_{\mathfrak{M}}\int\underset{\mathfrak{M}}{\cdots}\int |S_0|^{2t}\mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1$$
$$\ll P^{2k^2(1-(1-a)^n)}\cdot P^{2t-\frac{1}{2}k(k+1)} = P^{2t+2k^2(1-(1-a)^n)-\frac{1}{2}k(k+1)}.$$

又由第 10 章 §10.3 中的 7, 已知在 E 上

$$S_0 \ll P^{1-\lambda}, \quad \lambda = \frac{1}{50k^3\log k},$$

及引理 11.16,

$$\int\underset{E}{\cdots}\int |S_0|^{2t}\left|\prod_{j=1}^{n}\prod_{i=1}^{k}S_{ij}\right|^2 \mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1$$
$$\ll P^{2t(1-\lambda)}\int_0^1\cdots\int_0^1\left|\prod_{j=1}^{n}\prod_{i=1}^{k}S_{ij}\right|^2 \mathrm{d}\alpha_k\cdots\mathrm{d}\alpha_1$$
$$\ll P^{2t-2t\lambda+(2k^2-\frac{1}{2}k(k+1))(1-(1-a)^n)} \ll P^{2t+2t^2(1-(1-a)^n)-\frac{1}{2}k(k+1)}.$$

此处用了

$$\frac{1}{2}k(k+1)(1-a)^n \leqslant t(1-a)^n < 2t\lambda.$$

引理 11.17 已完全证明.

§11.6

对应地定义

$$\sigma_0(\alpha_k,\cdots,\alpha_1) = \sum_{p\leqslant 2P} e(\alpha_k p^k+\cdots+\alpha_1 p),$$
$$\sigma_{ij}(\alpha_k,\cdots,\alpha_1) = \sum_{(2i-1)P^{(1-a)^{j-1}}\leqslant p\leqslant 2iP^{(1-a)^{j-1}}} e(\alpha_k p^k+\cdots+\alpha_1 p),$$

$1\leqslant i\leqslant k, 1\leqslant j\leqslant n$. 命 $t=k^2+1$ 及

$$\Omega = \sigma_0^{2t+1}\prod_{j=1}^{n}\prod_{i=1}^{k}\sigma_{ij}^2 = \sum I'(N_k,\cdots,N_1)e(N_k\alpha_k+\cdots+N_1\alpha_1).$$

此处 $I'(N_k,\cdots,N_1)$ 是下列方程组的解的组数

$$\sum_{i=1}^{k}\sum_{j=1}^{n}p_{ij}^h + \sum_{i=1}^{k}\sum_{j=1}^{n}p_{ij}'^h + \sum_{v=1}^{2t+1}p_v''^h = N_h, \quad 1\leqslant h\leqslant k,$$

$$(2i-1)P^{(1-a)^{j-1}} \leqslant p_{ij}, p'_{ij} \leqslant 2iP^{(1-a)^{j-1}}, \quad 1 \leqslant p''_v \leqslant 2kP,$$

此处 $2kP = N_k^a$.

引理 11.18

$$I'(N_k, \cdots, N_1) = \frac{b_2 P^{2t+1+2k^2(1-(1-a)^n)-\frac{1}{2}k(k+1)} \mathfrak{S}(N_k, \cdots, N_1)}{L^{2t+1+2kn}} \times \left(1 + O\left(\frac{\log L}{L}\right)\right),$$

此处

$$b_2 = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \left\{ \left(\int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x) \mathrm{d}x \right)^{2t+1} \times \prod_{v=1}^{k} \left(\int_{(v-\frac{1}{2})a}^{va} e(\gamma_k x^k + \cdots + \gamma_1 x) \mathrm{d}x \right)^2 \times e\left(-\frac{N_k}{(2kP)^k}\gamma_k - \cdots - \frac{N_k}{2kP}\gamma_1 \right) \right\} \mathrm{d}\gamma_k \cdots \mathrm{d}\gamma_1.$$

证　我们有

$$I'(N_k, \cdots, N_1) = \int_0^1 \cdots \int_0^1 \sigma_0^{2t+1} \prod_{j=1}^{n} \prod_{i=1}^{k} \sigma_{ij}^2 e(-N_k\alpha_k - \cdots - N_1\alpha_1) \mathrm{d}\alpha_k \cdots \mathrm{d}\alpha_1.$$

如定理 16 的证明方法来分割积分范围. 由引理 10.8 及 11.17

$$\begin{aligned} &\int \underset{\mathfrak{N}}{\cdots} \int \left| \sigma_0^{2t+1} \prod_{j=1}^{n} \prod_{i=1}^{k} \sigma_{ij}^2 \right| \mathrm{d}\alpha_k \cdots \mathrm{d}\alpha_1 \\ &\ll PL^{-s^1} \int_0^1 \cdots \int_0^1 |\sigma_0|^{2t} \prod_{j=1}^{n} \prod_{i=1}^{k} |\sigma_{ij}|^2 \mathrm{d}\alpha_k \cdots \mathrm{d}\alpha_1 \\ &\ll PL^{-s^1} \int_0^1 \cdots \int_0^1 |S_0|^{2t} \prod_{j=1}^{n} \prod_{i=1}^{k} |S_{ij}|^2 \mathrm{d}\alpha_k \cdots \mathrm{d}\alpha_1 \\ &\ll P^{2t+1+2k^2(1-(1-a)^n)-\frac{1}{2}k(k+1)} L^{-s_1}. \end{aligned}$$

一如定理 16 的证明, 可证

$$\begin{aligned} &\sum_{\mathfrak{M}} \int_{\mathfrak{M}} \sigma_0^{2t+1} \prod_{i=1}^{k} \sigma_{i1}^2 e(-N_k\alpha_k - \cdots - N_1\alpha_1) \mathrm{d}\alpha_k \cdots \mathrm{d}\alpha_1 \\ &= b_2 \mathfrak{S}(N) P^{2t+2k+1-\frac{1}{2}k(k+1)} L^{-2t-2k-1} \left(1 + O\left(\frac{\log L}{L}\right)\right), \end{aligned}$$

此处

$$
\begin{aligned}
b_2 = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \Bigg\{ & \left(\int_0^1 e(\gamma_k x^k + \cdots + \gamma_1 x) \mathrm{d}x \right)^{2t+1} \\
& \times \prod_{v=1}^{k} \left(\int_{(v-\frac{1}{2})a}^{va} e(\gamma_k x^k + \cdots + \gamma_1 x) \mathrm{d}x \right)^2 \\
& \times e\left(-\frac{N_k}{(2kP)^k} \gamma_k - \cdots - \frac{N_1}{2kP} \gamma_1 \right) \Bigg\} \mathrm{d}\gamma_k \cdots \mathrm{d}\gamma_1 .
\end{aligned}
$$

再用引理 9.6 的证明中所用的方法, 可以得出我们所需要的定理.

第 12 章　其他的结果

§12.1

本章中将论及一些结果与问题, 这些都是可以藉助于本文中所叙述的方法而获得或解决的. 这些问题依其本性可以分成下列四个范畴:

a) 包含概念 “几乎一切” 或 “具有正密率” 的问题;

b) 由下列的假设而引导出来的问题: 即对于任何一个预定的整数 $N(>0)$, 必有一整数 A 存在, 使二次多项式

$$x^2-x+A.$$

当 $x=0,1,\cdots,N$ 时取素数值;

B) 把第十章的问题推广为若干不同多项式之和同时表示几个数的问题;

Γ) 由以下的推测所引导出的推论:

方程组

$$x_1^h+\cdots+x_{\frac{1}{2}k(k+1)}^h=y_1^h+\cdots+y_{\frac{1}{2}k(k+1)}^h,\quad 1\leqslant h\leqslant k,\quad 1\leqslant x,y\leqslant P,$$

有 $\ll c_1(k)P^{\frac{1}{2}k(k+1)}(\log P)^{c_2(k)}$ 组整数解.

有些不属于这些范畴的结果将在本章 §12.6 中论述之.

§12.2

假定 $\mathfrak{M}$ 是不同的自然数所成的集合, $M(x)$ 是其中不超过 x 的元素的个数. 又假定 $\mathfrak{N}$ 是集合 $\mathfrak{M}$ 的一个分集合, 而 $N(x)$ 是 $\mathfrak{N}$ 中不超过 x 的元素的个数. 如果

$$\lim_{x\to\infty}\frac{N(x)}{M(x)}=1,$$

则我们说: $\mathfrak{N}$ 几乎包含了 $\mathfrak{M}$ 的所有的元素. 特别是, 如果 $\mathfrak{M}$ 是由所有的 $\equiv l(\bmod q)$ 的正整数所组成的, 我们就简单地说: $\mathfrak{N}$ 几乎包含了一切 $\equiv l(\bmod q)$ 的整数.

又如果

$$\lim_{x\to\infty}\frac{M(x)}{x}\geqslant\alpha>0,$$

则我们说：$\mathfrak{M}$ 具有正的渐近密率.

设 $h(k)$ 表示满足下列条件的最小正整数 s, 即凡可表示成 s 个素数 k 次方的和的形状的整数所成的集合几乎包含一切 $\equiv s(\bmod K)$ 的正整数. 这 K 已在第 8 章中定义. 我们能够证明

$$h(1)=2, h(2)=3, h(3)\leqslant 5, h(4)\leqslant 8, h(5)\leqslant 13, h(6)\leqslant 20, h(7)\leqslant 28$$

及

$$h(k)\leqslant k+m+4,$$

这里 m 具有第 9 章 §9.1 的意义.

以 $f_v(x)$ 代表 s_0 个 k 次整值多项式, 而 s_0 的定义是

k	1	2	3	4	5	6	7	8	9	10	$\geqslant 11$
s_0	2	3	5	8	13	20	28	36	45	55	$k+m+4$

则能表成

$$f_1(p_1)+\cdots+f_s(p_s)\quad (p\text{是素数})$$

形式的整数集合有正的渐近密率.

§12.3 一个假设的陈述

对任意预给的整数 $N(>0)$, 必有一整数 A 存在使

$$x^2-x+A$$

当 $x=0,1,\cdots,N$ 时表示素数. 以下的数据支持了这一假设的真确性：当 $x=0,1,\cdots,40$ 时

$$x^2-x+41$$

代表素数. 又

$$x^2-x+19421, x^2-x+27941, x^2-x+72491$$

都代表丰富的素数 (最后一个由 $x=0$ 到 $x=11000$ 都代表素数)*.

换一种说明的方法：有 $N+1$ 个方程, $N+1$ 个素数未知数 $p_m(0\leqslant m\leqslant N)$ 及 A 使

$$m^2-m+A=p_m,\quad 0\leqslant m\leqslant N,$$

* Beeger, N. G. W. H., Report on some calculations of prime numbers, *Nieuw. Arch. Wiskde*, **20**(1939), 40-50.

可解. 消去未知数 A, 则得

$$m^2-m=p_m-p_0,\quad 1\leqslant m\leqslant N,$$

即得一方程组其中有 N 个方程及 $N+1$ 个素数未知数. 把这一问题提高到更一般性: 就是求解一组 N 个联立方程其中有 $N+1$ 个素数未知数的问题:

$$\sum_{j=1}^{N+1}a_{ij}p_j=b_i,\quad 1\leqslant i\leqslant N. \tag{1}$$

当然要这问题有解必需要有"正可解条件"和"同余可解条件", 但在今天这一问题的解答还在数学家的能力之外, 而我们所可能为力者在证明: 对几乎所有的适合同余可解条件的 b, (1) 式可解.

但方程组

$$\sum_{j=1}^{2N+1}a_{ij}p_j=b_i,\quad 1\leqslant i\leqslant N$$

在正可解及同余可解条件下对所有的充分大的 b 是可解的.

最后举出本问题中所包有的若干有趣的特例:

Ⅰ) 哥德巴赫问题: 方程

$$p_1+p_2=2n.$$

当 $n>1$ 时可解. (此即以上一般性的问题为 $N=1$ 时的特例).

Ⅱ) 孪生素数问题: 方程

$$p_1-p_2=2$$

有无穷个解.

Ⅲ) 三生素数问题: 方程组

$$p_1-p_2=2,\quad p_2-p_4=4$$

有无穷个解 (或

$$p_1-p_2=4,\quad p_2-p_4=2$$

有无穷个解).

§12.4　第 10 章及第 11 章的方法用到更普遍的问题

命 $\{f_{i1}(x),\cdots,f_{is}(x)\}(1\leqslant i\leqslant k)$ 表 k 组, 每一组有 s 个整值多项式. 现在的问题是解方程组

$$f_{11}(p_1)+\cdots+f_{1s}(p_s)=N_1,$$

$$\cdots\cdots$$

$$f_{k1}(p_1)+\cdots+f_{ks}(p_s)=N_k.$$

这一类方程的解答并不太难, 如果我们假定 f 的次数是受囿的, 且 s 是相当大的话. 一般说来, 第 10 及第 11 章的方法可用, 但须引进以下的不等式:

$$\int\cdots\int|g_1\cdots g_s|\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\leqslant\left(\prod_{v=1}^{s}\int\cdots\int|g_v|^s\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\right)^{1/s}.$$

§12.5　一假设的叙述

假设: 方程组

$$x_1^h+\cdots+x_{\frac{1}{2}k(k+1)}^h=y_1^h+\cdots+y_{\frac{1}{2}k(k+1)}^h,\quad 1\leqslant h\leqslant k,\quad 1\leqslant x,\quad y\leqslant P$$

的整数解的组数 $\leqslant c_1(k)P^{\frac{1}{2}k(k+1)}(\log P)^{c_2(k)}$.

这一假设的真实性, 当 $k=1$ 时, 十分显然. 当 $k=2$ 时, 已在第 4 章中证明了 (定理 B_2'). 当 $k\geqslant 3$ 时, 这是一留待解决的问题. 如果能证明此点, 则本书中一切的定理都可以改善. 例如: 解数的渐近式将当 $s>\dfrac{1}{2}k(k+1)$ 时真实. 这一假设的证实在解析数论中还有其他的很多应用.

§12.6

本节中再叙述一些其他的结果:

Ⅰ) 所有的充分大的整数可以表成一个素数及 s 个素数的 k 次方的和, 如果 $s\geqslant s_0\sim 2k\log k$.

Ⅱ) 所有的充分大的整数可以表成一个素数及 s 个整数的 k 次方之和, 如果 $s\geqslant s_0\sim\dfrac{3}{2}k\log k$.

Ⅲ) 所有的充分大的整数可以表成 s 个不多于两个素因子的整数的 k 乘方的和, 如果 $s\geqslant s_0\sim 3k\log k$.

关于Ⅱ) 及Ⅲ) 的证明方法必须采用维诺格拉陀夫的另一创造必的方法, 见 Виноградов, Метод тригонометрических сумм в теории чисел, Труды Матем. *uиcmumymа* им. В. А. Стекдова, т. 23, стр. 1-109, 特别是其中的第 4 章.

附　　录

命 $f(x)$ 为一 k 次实系数多项式, 或为一在某种意义下能以 k 次多项式密切逼近的实函数, 又命

$$S = \sum_{x=Q+1}^{Q+P} e^{2\pi i f(x)}.$$

在将这种三角和的估计应用于解析数论的研究时, k 往往与 P 同时趋向无穷. 因此为了使结果更为精密, 就必须考虑 Виноградов 中值定理中与 k 有关的常数因子的改进. 更确切地说, 我们将证明

定理　命 $l \geqslant 1$, 则当

$$\frac{1}{3}k(k+1) + lk \leqslant s \leqslant 4k^2 \log k$$

时, 将有

$$\int_0^1 \cdots \int_0^1 |C_k(P)|^{2s} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \leqslant k^{9k^3} \mathrm{e}^{23k^2 l} \log^l P \cdot P^{2s-\frac{1}{2}k(k+1)+\delta_l},$$

此处

$$\delta_l = \frac{1}{2}k(k+1)(1-a)^l, \quad a = \frac{1}{k}.$$

定理的证明与定理 5′ 的证明很相类似. 但在这里我们将用下面的二个引理来代替引理 4.1 与 4.2.

引理 1　命 $Q = RH, R > 1, H > 1$ 及

$$1 \leqslant g_1 < g_2 < \cdots < g_k \leqslant H, \quad g_v - g_{v-1} > 1, \tag{1}$$

此处 $g_1, \cdots, g_k$ 是整数. 又命 x_v 在隔间

$$-\omega + (g_v - 1)R < x_v \leqslant -\omega + g_v R, \quad 0 \leqslant \omega \leqslant Q \tag{2}$$

中变化. 则整数组 $x_1, \cdots, x_k$ 中使

$$x_1^h + \cdots + x_k^h, \quad 1 \leqslant h \leqslant k$$

各落在长度 $\leqslant Q^{h-1} (1 \leqslant h \leqslant k)$ 的隔间中的组数

$$\leqslant \mathrm{e}^{3k^2} k^{-\frac{1}{2}k^2} H^{\frac{1}{2}k(k-1)}. \tag{3}$$

证　设 h 为适合 $1 < h \leqslant k$ 的整数. 给定 $x_{h+1}, \cdots, x_k$, 并假定 $x_1, \cdots, x_h$ 及 $y_1, \cdots, y_h$ 为二组整数使 $x_1^r + \cdots + x_k^r$ 及 $y_1^r + \cdots + y_h^r + x_{h+1}^r + \cdots + x_k^r$ 同时落入一组长度不超过 $Q^{r-1}(1 \leqslant r \leqslant k)$ 的隔间中者. 于是

$$x_1^r + \cdots + x_h^r - (y_1^r + \cdots + y_h^r) = \theta_r Q^{r-1}, \quad 1 \leqslant r \leqslant h,$$

亦即

$$\frac{x_1 - y_1}{x_1 - y_1}(x_1 - y_1) + \cdots + \frac{x_h - y_h}{x_h - y_h}(x_h - y_h) = \theta_1,$$
$$\cdots\cdots$$
$$\frac{x_1^h - y_1^h}{x_1 - y_1}(x_1 - y_1) + \cdots + \frac{x_h^h - y_h^h}{x_h - y_h}(x_h - y_h) = \theta_h Q^{h-1},$$

而 $|\theta_r| \leqslant 1$. 将 $x_1 - y_1, \cdots, x_h - y_h$ 视为变数, 而解此线性方程组, 得到

$$\varDelta(x_h - y_h) \pm \varDelta' = 0, \tag{4}$$

其中

$$\varDelta = \begin{vmatrix} \dfrac{x_1 - y_1}{x_1 - y_1} & \cdots & \dfrac{x_h - y_h}{x_h - y_h} \\ \cdots & \cdots & \cdots \\ \dfrac{x_1^h - y_1^h}{h(x_1 - y_1)} & \cdots & \dfrac{x_h^h - y_h^h}{h(x_h - y_h)} \end{vmatrix},$$

$$\varDelta' = \begin{vmatrix} \dfrac{x_1 - y_1}{x_1 - y_1} & \cdots & \dfrac{x_{h-1} - y_{h-1}}{x_{h-1} - y_{h-1}} & \theta_1 \\ \cdots & \cdots & \cdots & \cdots \\ \dfrac{x_1^h - y_1^h}{h(x_1 - y_1)} & \cdots & \dfrac{x_{h-1}^h - y_{h-1}^h}{h(x_{h-1} - y_{h-1})} & \dfrac{\theta_h}{h} Q^{h-1} \end{vmatrix}.$$

将 (4) 式改写成

$$\frac{1}{\displaystyle\prod_{r=1}^{h}(x_r - y_r)} \int_{y_1}^{x_1} \cdots \int_{y_h}^{x_h} \{\varDelta_h(x_h - y_h) \pm \varDelta_h'\} \mathrm{d}z_1 \cdots \mathrm{d}z_h = 0,$$

此处

$$\varDelta_h = \begin{vmatrix} 1 & \cdots & 1 \\ z_1 & \cdots & z_h \\ \cdots & \cdots & \cdots \\ z_1^{h-1} & \cdots & z_h^{h-1} \end{vmatrix}, \quad \varDelta_h' = \begin{vmatrix} 1 & \cdots & 1 & \theta_1 \\ z_1 & \cdots & z_{h-1} & \dfrac{1}{2}\theta_2 Q \\ \cdots & \cdots & \cdots & \cdots \\ z_1^{h-1} & \cdots & z_{h-1}^{h-1} & \dfrac{1}{h}\theta_k Q^{h-1} \end{vmatrix}.$$

于是应用积分的中值定理可知：必有一组 $z_1, \cdots, z_h$，使

$$\Delta_h(x_h - y_h) \pm \Delta'_h = 0. \tag{5}$$

因

$$\Delta_h = \Delta_{h-1}(z_h - z_1)\cdots(z_h - z_{h-1}),$$

命 σ_{h-r} 表 $z_1, \cdots, z_{h-1}$ 的 $h-r$ 次初等对称函数，显然有 $|\sigma_{h-r}| \leqslant \binom{h-1}{h-r} Q^{h-r}$. 故在 Δ_h 的展开式中，z_h^{r-1} 的系数的绝对值

$$= |\sigma_{h-r}\Delta_{h-1}| \leqslant \binom{h-1}{r-1} Q^{h-r}|\Delta_{h-1}|.$$

于是

$$|\Delta'_h| \leqslant |\Delta_{h-1}|\sum_{r=1}^{h}\frac{|\sigma_{h-r}|}{r}Q^{r-1} \leqslant |\Delta_{h-1}|Q^{h-1}\sum_{r=1}^{h}\frac{1}{r}\binom{h-1}{r-1},$$

因此得到

$$|x_h - y_h| \leqslant \frac{Q^{h-1}\sum_{r=1}^{h}\frac{1}{r}\binom{h-1}{r-1}}{(z_h - z_1)\cdots(z_h - z_{h-1})} \leqslant \frac{2^h Q^{h-1}}{R(3R)\cdots((2h-3)R)}$$
$$= \frac{2^h H^{h-1}}{1\cdot 3\cdots(2h-3)} = L_h.$$

因此对于给定的 $x_{h+1}, \cdots, x_k, x_h$ 至多能取 $L_h + 1 \leqslant 2L_h$ 个不同的值. 故适合引理要求的整数组 $x_1, \cdots, x_k$ 的组数不能超过

$$2\prod_{h=2}^{k}\frac{1}{1\cdot 3\cdots(2h-3)}\prod_{h=2}^{k}2^{h+1}\cdot H^{\frac{1}{2}k(k-1)}.$$

利用极显然的不等式

$$\sum_{n=1}^{N}\log n \geqslant \int_1^N \log x\mathrm{d}x$$

及

$$\sum_{n=1}^{N} n\log n \geqslant \int_1^N x\log x\mathrm{d}x$$

不难得出引理.

引理 2　命 $c \geqslant 1$. 在引理 1 的假定下，整数组 $x_1, \cdots, x_k$ 中，使

$$x_1^h + \cdots + x_k^h, \quad 1 \leqslant h \leqslant k$$

各落在长不超过 $cQ^{(1-a)h}(1\leqslant h\leqslant k)$ 中的组数不超过

$$(2c)^k e^{3k^2} k^{-\frac{1}{2}k^2} H^{\frac{1}{2}k(k-1)} Q^{\frac{1}{2}(k-1)}. \tag{6}$$

证明与引理 4.2 相同.

引理 3　设 s 为一适合 $2^s\leqslant \dfrac{Q}{(2k-1)(Q^{1-a}-1)}$ 的整数. 命 $H_s=2^s(2k-1), R_s=Q/H_s$. 又命

$$Z_{sg_i}=\sum_{(g_i-1)R_s<x\leqslant g_iR_s} e(f(x)),\quad 1\leqslant i\leqslant k$$

及

$$C^*=\sum_{\omega<x\leqslant\omega+Q'} e(f(x)),$$

此处 $0<Q'\leqslant Q^{1-a}$ 及 $0\leqslant\omega\leqslant Q$. 则当 $g_1,\cdots,g_k$ 为一佳位组时

$$\begin{aligned}&\int_0^1\cdots\int_0^1 |Z_{sg_1}\cdots Z_{sg_k}|^2|C^*|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant\ & b^k e^{4k^2} 2^{s[\frac{1}{2}k(k-1)-k]} Q^{2k-\frac{1}{2}(k+1)}\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.\end{aligned} \tag{7}$$

引理之证明与引理 4.4 部分 3) 中所用的方法相同.

引理 4　(递推公式). 命 b 为一适合

$$\frac{1}{3}k(k+1)+k<b\leqslant 4k^2\log k \tag{8}$$

的整数. 若

$$\log Q>4k\log(4k), \tag{9}$$

则

$$\begin{aligned}&\int_0^1\cdots\int_0^1 |C_k(Q)|^{2b}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k\\ \leqslant\ & e^{23k^2} Q^{2k-\frac{1}{2}(k+1)+2(b-k)a}\log Q\int_0^1\cdots\int_0^1 |C_k(Q^{1-a})|^{2(b-k)}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.\end{aligned} \tag{10}$$

证　命 η 为由下式所确定的整数:

$$2^{\eta-1}\leqslant\frac{Q}{(2k-1)(Q^{1-a}-1)}<2^\eta. \tag{11}$$

由引理之假定, 显见 $\eta\geqslant 4$.

分 $C_k(Q)$ 为 $H_s = 2^s(2k-1)$ 部分, 每份之长度为 $R_s = Q/H_s$. 则用与引理 4.4 相同的方法. 可以得到

$$|C_k(Q)|^{2b} \leqslant 2\eta \sum_{s=0}^{\eta} M_s \sum^{M_s} |Z_s'|^2, \tag{12}$$

此处 Z_s', 与 M_s 的意义与引理 4.4 中相同, 但

$$M_s = H_s^{k-1}(4(k-1))^b, \quad s > 0, \quad M_0 \leqslant (2k-1)^b.$$

当 $0 \leqslant s \leqslant \eta - 1$ 时, 与引理 4.4 相同地可以证明

$$\begin{aligned}|Z_s'|^2 &\leqslant \frac{1}{b-k} \sum_{i=k+1}^{b} |Z_{sg_1} \cdots Z_{sg_k}|^2 |Z_{sg_i}|^{2(b-k)} \\ &\leqslant \frac{1}{b-k} \sum_{i=k+1}^{b} N_s^{2(b-k)-1} \sum^{N_s} |Z_{sg_1} \cdots Z_{sg_k}|^2 |C^*|^{2(b-k)},\end{aligned}$$

其中

$$\begin{aligned}N_s &= \left[\frac{Q}{2^s(2k-1)} \frac{1}{Q^{1-a}-1}\right] + 1 \\ &\leqslant \begin{cases} \dfrac{Q^a}{2^{s+1}(k-1)}, & s = 0,1,2, \\ \dfrac{Q^a}{2^s(k-1)}, & 3 \leqslant s \leqslant \eta - 1. \end{cases}\end{aligned}$$

于是由引理 3 及以上诸式得

$$\begin{aligned}&\int_0^1 \cdots \int_0^1 \sum_{s=0}^{\eta-1} M_s \sum^{M_s} |Z_s'|^2 \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \\ \leqslant{}& k^{17k} e^{6k^2} Q^{2k-\frac{1}{2}(k+1)+2(b-k)a} \int_0^1 \cdots \int_0^1 |C_k(Q^{1-a})|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k.\end{aligned} \tag{13}$$

当 $s = \eta$ 时, 由 (11) 式得到

$$\begin{aligned}|Z_\eta'|^2 &\leqslant \frac{1}{b-k} \sum_{i=k+1}^{b} |Z_{\eta g_1} \cdots Z_{\eta g_k}|^2 |Z_{\eta g_i}|^{2(b-k)} \\ &\leqslant R_\eta^{2k} |C^*|^{2(b-k)},\end{aligned}$$

故由 (9) 式得

$$\int_0^1 \cdots \int_0^1 M_\eta \sum^{M_\eta} |Z_\eta'|^2 \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k$$

$$\leqslant M_\eta^2 R_\eta^{2k} \int_0^1 \cdots \int_0^1 |C_k(Q^{1-a})|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k$$

$$\leqslant (4k)^{2k} Q^{2k-\frac{1}{2}(k+1)+2(b-k)a} \int_0^1 \cdots \int_0^1 |C_k(Q^{1-a})|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k. \tag{14}$$

因 $\eta \leqslant \log Q$, 及 (12), (13), (14) 诸式, 而引理得证.

定理的证明：令 l_0 为由下式所确定的整数：

$$(1-a)^{-(l_0-1)} 4k \log(4k) < \log P \leqslant (1-a)^{-l_0} 4k \log(4k).$$

若 $l_0 \geqslant l$ 时, 可以证明

$$\int_0^1 \cdots \int_0^1 |C_k(P)|^{2s} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \leqslant \mathrm{e}^{23k^2 l} \log^l P \cdot P^{2s-\frac{1}{2}k(k+1)+\delta_l}, \tag{15}$$

事实上, 当 $l=0$ 时, (15) 式是显然的. 对于 $l>0$ 的情形, 可由引理 4, 并对 l 实行数学归纳法而得到.

若 $1 \leqslant l_0 < l$, 由 (15) 式可以得到

$$\int_0^1 \cdots \int_0^1 |C_k(P)|^{2s} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \leqslant \mathrm{e}^{23k^2 l_0} \log^{l_0} P \cdot P^{2s-\frac{1}{2}k(k+1)+\delta_{l_0}},$$

则因

$$P^{\delta_{l_0}} = P^{\frac{1}{2}k(k+1)(1-a)^{l_0}} \leqslant (4k)^{4k\cdot\frac{1}{2}k(k+1)} \leqslant k^{9k^3},$$

而得定理.

对于 $l_0 < 1 \leqslant l$ 的情形, 则由

$$P^{\frac{1}{2}k(k+1)} \leqslant (4k)^{4k\cdot\frac{1}{2}k(k+1)} \leqslant k^{9k^3},$$

故

$$\int_0^1 \cdots \int_0^1 |C_k(P)|^{2s} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \leqslant P^{2s} \leqslant k^{9k^3} P^{2s-\frac{1}{2}k(k+1)},$$

而定理证毕.

主要引理　命

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x + \alpha_0$$

为一实系数的 k 次多项式, 而命 P 为一适合

$$2k|\alpha_k|P \leqslant 1$$

的正整数. 则

$$\sum_{x=Q+1}^{Q+P} \mathrm{e}^{2\pi \mathrm{i} f(x)} = 0(\mathrm{e}^{32k} P^{1-\frac{A}{k^2 \log k}} \log P) + O(|\alpha_k|^{-\frac{1}{k-1}}),$$

此处 A 与符号 O 内所含的常数都是绝对常数.

证　若 $|\alpha_k|^{-\frac{1}{k-1}} \geqslant P$, 则引理显然. 故不妨假定

$$|\alpha_k|^{-\frac{1}{k-1}} < P.$$

命 Y 为一适合 $2 \leqslant Y \leqslant P$ 的常数, 而命

$$S = \sum_{x=Q+1}^{Q+P} e(f(x)), \quad S_1(x) = \sum_{y=1}^{Y} e(f(x+y)),$$

则

$$\sum_{x=Q+1}^{Q+P}\sum_{y=1}^{Y} e(f(x+y)) = Y \sum_{m=Q+Y+1}^{Q+P} e(f(m)) + \left(\sum_{m=Q+2}^{Q+Y} + \sum_{m=Q+P+1}^{Q+P+Y}\right) O(Y) = YS + O(Y^2),$$

亦即

$$S = \frac{1}{Y}\sum_{x=Q+1}^{Q+P} S_1(x) + O(Y).$$

所以由Hölder不等式, 得到

$$S \ll \frac{1}{Y}\left(P^{2s-1}\sum_{x=Q+1}^{Q+P} |S_1(x)|^{2s}\right)^{\frac{1}{2s}} + Y.$$

命

$$f(x+y) = A_k y^k + A_{k-1} y^{k-1} + \cdots + A_0,$$

此处 $A_k = \alpha_k, A_{k-1} = \alpha_{k-1} + k\alpha_k x$. 于是

$$|S_1(x)|^{2s} = \sum_{y_1=1}^{Y}\cdots\sum_{y_s=1}^{Y}\sum_{y_1'=1}^{Y}\cdots\sum_{y_s'=1}^{Y} e(\Phi)$$

此处

$$\begin{aligned}\Phi &= f(x+y_1) + \cdots + f(x+y_s) - f(x+y_1') - \cdots - f(x+y_s') \\ &= \sum_{h=1}^{k} A_h (y_1^h + \cdots + y_s^k - y_1'^h - \cdots - y_s'^h).\end{aligned}$$

命 $\psi(N_1,\cdots,N_{k-1})$ 表示下列方程组的整数解组数:

$$y_1^h+\cdots+y_s^h-y_1'^h-\cdots-y_s'^h=N_h,\quad 1\leqslant h\leqslant k-1,$$
$$1\leqslant y,y'\leqslant Y,$$

则因 A_k 与 x 无关, 故可得

$$\sum_{x=Q+1}^{Q+P}|S_1(x)|^{2s}\leqslant\sum_{y_1=1}^{Y}\cdots\sum_{y_s=1}^{Y}\sum_{y_1'=1}^{Y}\cdots\sum_{y_s'=1}^{Y}\left|\sum_{x=Q+1}^{Q+P}e(\varPhi)\right|$$
$$=\sum_{N_1=-2sY}^{2sY}\cdots\sum_{N_{k-1}=-2sY^{k-1}}^{2sY^{k-1}}\psi(N_1,\cdots,N_{k-1})\left|\sum_{x=Q+1}^{Q+P}e(A_{k-1}N_{k-1}+\cdots+A_1N_1)\right|.$$

由Cauchy不等式, 得到

$$\sum_{x=Q+1}^{Q+P}|S_1(x)|^{2s}\leqslant\left(\sum_{N_1}\cdots\sum_{N_{k-1}}\psi^2(N_1,\cdots,N_{k-1})\right)^{\frac12}$$
$$\left(\sum_{N_1}\cdots\sum_{N_{k-1}}\left|\sum_{x=Q+1}^{Q+P}e(A_{k-1}N_{k-1}+\cdots+A_1N_1)\right|^2\right)^{\frac12}.$$

因

$$\sum_{N_1}\cdots\sum_{N_{k-1}}\psi^2(N_1,\cdots,N_{k-1})$$

等于下列方程组

$$y_1^h+\cdots+y_s^h-y_1'^h-\cdots-y_s'^h=z_1^h+\cdots+z_s^h-z_1'^h-\cdots-z_s'^h,$$
$$1\leqslant h\leqslant k-1,\quad 1\leqslant y,y',z,z'\leqslant Y$$

的整数解组数, 也就是

$$\int_0^1\cdots\int_0^1|C_{k-1}(Y)|^{4s}\mathrm{d}\alpha_1\cdots\mathrm{d}\alpha_k.$$

故由定理得到

$$\sum_{N_1}\cdots\sum_{N_{k-1}}\psi^2(N_1,\cdots,N_{k-1})\leqslant k^{9k^3}\mathrm{e}^{23k^2l}\log^l Y\cdot Y^{4s-\frac12k(k-1)+\delta_l}.$$

又

$$\sum_{N_1}\cdots\sum_{N_{k-1}}\left|\sum_{x=Q+1}^{Q+P}e(A_{k-1}N_{k-1}+\cdots+A_1N_1)\right|^2$$

$$\leqslant \sum_{N_1}\cdots\sum_{N_{k-2}}\sum_{x_1=Q+1}^{Q+P}\sum_{x_2=Q+1}^{Q+P}\left|\sum_{N_{k-1}=-2SY^{k-1}}^{2SY^{k-1}} \mathrm{e}^{2\pi i k\alpha_k(x_1-x_2)N_{k-1}}\right|$$

$$\leqslant (5s)^{k-1}Y^{\frac{1}{2}(k-1)(k-2)}\sum_{x_1=Q+1}^{Q+P}\sum_{x_2=Q+1}^{Q+P}\min\left(5sY^{k-1},\frac{1}{\{k\alpha_k(x_1-x_2)\}}\right)$$

$$\leqslant (5s)^{k-1}Y^{\frac{1}{2}(k-1)(k-2)}P\sum_{x=-P}^{P}\min\left(5sY^{k-1},\frac{1}{\{k\alpha_k x\}}\right)$$

$$\leqslant (5s)^{k-1}Y^{\frac{1}{2}(k-1)(k-2)}P\left(5sY^{k-1}+\frac{2}{k|\alpha_k|}\sum_{x=1}^{P}\frac{1}{x}\right)$$

$$\leqslant (5s)^{k}Y^{\frac{1}{2}(k-1)(k-2)}P\left(Y^{k-1}+\frac{1}{k|\alpha_k|}\log P\right).$$

由以上诸式, 立刻得到

$$S\ll P^{1-\frac{1}{2s}}\left(k^{9k^3}\mathrm{e}^{23k^2l}\log^l Y\cdot Y^{-(k-1)+\delta_l}(5s)^kP\left(Y^{k-1}+\frac{\log P}{k|\alpha_k|}\right)\right)^{\frac{1}{4s}}+Y.$$

取 $s=[(k-1)^2\log(k-1)]$, 易证 $\delta_l\leqslant\dfrac{1}{2}$. 故得

$$S\ll \mathrm{e}^{32k}\log P\cdot P^{1-\frac{1}{4s}}\left(Y^{-(k-1)+\frac{1}{2}}\left(Y^{k-1}+\frac{1}{|\alpha_k|}\right)\right)^{\frac{1}{4s}}+Y.$$

取

$$Y=\begin{cases}[|\alpha_k|^{-\frac{1}{k-1}}], & 若 2^{k-1}\leqslant|\alpha_k|^{-1},\\ [P^{1-\frac{1}{10s}}], & 若 2^{k-1}>|\alpha_k|^{-1}\end{cases}$$

而引理得证.

这一引理在解析数论中有着重要的意义. 下面我们叙述它的几个应用, 这些应用都可以从主要引理及已知的方法无须经过重大的改变而得到.

1) $\zeta(1+it)=O(\log^{\frac{3}{4}}t\log\log^{\frac{1}{4}}t)$[1].

2) $\pi(x)=\mathrm{li}x+O(x^{-A\log^{\frac{4}{7}-\varepsilon}x})$[1].

3) 中值公式

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T|\zeta(\sigma+it)|^{2k}\mathrm{d}t=\sum_{n=1}^{\infty}d_k^2(n)n^{-2\sigma}$$

---

[1] 华罗庚与吴方: Виноградов 中值定理的一个改进和它的某些应用. 数学学报 7 卷 3 期

之有效区域 [2].

4) 设 $A(x)$ 为椭球体

$$\sum_{i,j=1}^{4} a_{ij}x_ix_j \leqslant x \quad (a_{ij}=a_{ji}\text{为整数})$$

内的整点数, D 为此二次形式的行列式. 则

$$A(x)-\frac{\pi^2}{2\sqrt{D}}x^2=O(x\log^{\frac{3}{4}}x\log\log^{\frac{1}{4}}x)^{[3]}.$$

[2] Davenport, Journal of London Math. Soc., 10(1935), 136-138.

[3] Walfisz, Travaux de l'institut mathématique de Tbilisi, 5(1938), 181-196.

（华罗庚文集数论卷 I · 下部）

指数和的估计及其在数论中的应用[1]

① 本部分内容曾作为著作出版，见《指数和的估计及其在数论中的应用》，北京：科学出版社，1963 年.

序[①]

"指数和的估计及其在数论中的应用" 一书是应 "德国数学百科全书" 编委会之请而写, 作为这套书的一个分册于 1959 年在德国以德文出版.

本书的目的在于系统地总结指数和方法. 近代解析数论、几何数论与堆垒数论所以有如此重大的发展, 都是由于指数和方法的引入与改进. 尤其是著名的素数分布问题, Waring 问题, Гольдбах 问题, Tarry 问题以及圆内、球内整点问题等, 更加如此.

作为百科全书的一部分, 本书力求较全面地介绍这一分支的工作. 不仅如此, 本书的写作方法, 还不只是结果与文献的罗列, 而是尽力注意到这一分支的系统性、关联性与完整性. 我试图把主要结果贯穿起来, 并且尽可能地扼要地涉及到这些结果的证明. 希望有一定数学修养的读者, 可以直接看懂本书的主要部分, 而不必另翻原作. 以上是作者平素对总结性与综合性文章的撰写要求, 虽然由于篇幅有限以及作者知识水平的局限, 未能完全如愿, 但作者还是尽力为之的.

本书由 1952 年开始撰写, 至 1956 年完稿, 自始至终是在中国科学院数学研究所党组织的支持与鼓励下进行工作的. 饮水思源, 衷心感谢. 在写作过程中, 很多同志帮我查阅了可能得到的文献, 并且编制了附有摘要的文献卡片. 而本书就是在掌握这些材料之后, 经整理、消化、取舍与综合, 而后写成的. 王元与吴方两同志将本书译成了中文. 作者谨向这些同志致以谢意.

最后, 作者衷心地希望读者多提意见与批评.

华罗庚

1963 年 1 月

① 取自《指数和的估计及其在数论中的应用》.

导　引①

堆垒数论的历史是从两个著名的问题, 即Гольдбах 问题与 Waring 问题开始的.

Гольдбах 问题是在 1742[1] 年, Гольдбах 写信给 Euler 时提出的. 在信中, Гольдбах 提出了关于将整数表为素数和的两个猜想. 这两个猜想可用略为修改了的语言叙述为: (A) 每一个 $\geqslant 6$ 的偶数都是两个奇素数之和; (B) 每一个 $\geqslant 9$ 的奇数都可以表成三个奇素数之和. 显然, 由命题 (A) 可以推出命题 (B).

从Гольдбах 写信起到今天, 已经积累了不少宝贵的数值资料 [2]. 这些资料指出了这两个猜想是正确的, 但迄今还不能证明它们的真伪.

大约在四十年前 [3], 即使是证明如下的命题: 存在的一个整数 c, 使每一个 $\geqslant 2$ 的整数都可表为不超过 c 个素数之和, 也被认为是现代数学家力所不能及的事.

在 1770 年, Waring 提出了下面的猜想 [4]: 每一个自然数都是四个平方之和, 九个立方之和, 十九个四方之和, 等等. 他的言论表明了他相信: 对于每一个给定的整数 $k \geqslant 2$, 恒存在一仅依赖于 k 的整数 $s = s(k)$, 使每一正整数都可表为不超过 s 个非负整数的 k 次方之和.

Hilbert[5] 在 1909 年 (Waring 提出猜想后的 139 年) 首先证明了 $s(k)$ 的存在性. 以后, Шнирельман[6] 又在 1930 年 (Гольдбах 提出猜想后的 188 年) 证明了 c 的存在性. Hilbert 的方法虽然是很奇妙的, 但它在堆垒素数论的近代发展中, 并未显示出其功效. 但另一方面, Шнирельман 方法是广有用途的. 我们可以用这一方法同时处理这两个问题. 更须指出, 在Шнирельман 的论文中, 他引入了关于自然数集合的非常重要的概念 —— “正密率”.

Hardy 与 Littlewood 在这一世纪的二十年代, 作出了极为重要的贡献. 用他们强有力的方法, 不仅能够得到关于存在性的结果, 而且可以得到明确的上界. 在总标题为“‘partitio numerorum’的若干问题”[7] 的一系列论文中, 他们系统地开创与发展了堆垒数论中的一个崭新的解析方法. 这个方法就是人所共知的 Hardy 与 Littlewood 的圆法 [8]. 命 $G(k)$ 表示最小的整数 s, 使每一充分大的整数都能表成 s 个非负整数的 k 次方之和. 圆法可以得出 $G(k)$ 的一个明确的上界. 同时他们在广义 Riemann 猜想之下, 证明了每一充分大的奇数都可以表为三个素数之和. Landau[9] 把这些结果都很好地整理在他的专著之中了.

---

① 取自《指数和的估计及其在数论中的应用》.

为了取消在证明Гольдбах 问题时所用到的未经证明的猜想, 并改进 Waring 问题中的上界 $G(k)$, 我们需要估计某种类型的指数和 (Виноградов 称它们为三角和). 因此, 获得指数和的精确估计就成了近代堆垒数论的解析方法发展中的最主要环节了. 在近三十年来, Виноградов 创造了一系列估计指数和的天才方法. 因此, 他对 Hardy-Littlewood 方法作了巨大的改进.

对于Гольдбах 问题, Виноградов 成功地对某种以素数为变数的指数和给出了非无聊的估计, 他证明 [10] 了命题 (B) 对于充分大的奇数是正确的. Бороздкий[11] 经过计算证明了, 每一奇数 $n \geqslant \mathrm{e}^{\mathrm{e}^{16.038}}$ 都能表成三个奇素数之和.

后来, Линник[12] 沿用 Hardy-Littlewood 原来的方法, 并借助于 Dirichlet L- 函数的零点的知识, 亦证明了同样的结果.

另外一个研究Гольдбах 问题的方法就是"筛法". 这一方法是 Erathostenes[13] 首创的. Brun[14] 与 Selberg[15] 分别对这一方法作出了重要的改进. 由这一方法所得到的最好的、已经发表的结果是 [16]：每一充分大的偶数都是两个素因子个数各不超过 3 的整数之和. 但是无论如何, Selberg[17] 曾经宣布过, 用他的方法可能证明每一充分大的偶数都可表为一个不超过 2 个素数的乘积及一个不多于 3 个素数的乘积之和. 此外, 应用Линник[18] 的大筛法, Renyi[19] 证明了：每一充分大的偶数都是一个素数及一个素因子个数不超过某一给定常数的整数之和.

我们称在 Waring 问题的研究中所遇到的指数和为 Weyl 和. Weyl[20] 在关于一致分布的开创性工作中, 最先使用了这种和. 因此, 他也是首先给出这种和以非无聊估值的人. 他的估计成了 Hardy-Littlewood 关于 Waring 问题的研究方法中的一个最主要环节. Виноградов 与 van der Corput 作出了关于估计这种和的重要贡献.

Виноградов[21] 在 1935 年发表了一系列关于 Weyl 和的论文, 他不断地改进着自己的结果. 他的方法的最后形式被收集在他的选集 [22] 之中. 在华罗庚 [23] 的专著中也有着Виноградов 方法的略为改进了的形式. Виноградов 方法的价值不仅在于它能成功地用于 Waring 问题, 而且它还有效地应用于素数分布论, Riemann ζ- 函数论及 Dirichlet L- 函数论, 一致分布及 Diophantine 逼近论, 高维椭球中的格子点估计及 Prouhet 问题等等. 例如, 用Виноградов 的结果可以证明, 不超过 x 的素数个数等于

$$\mathrm{li}\, x + O(x\mathrm{e}^{-c(\log\, x)^{3/5}})\text{[24]}.$$

我们称下面的问题为 Prouhet 问题 [25] (有时也称为 Tarry 问题或 Tarry-Escott 问题), 即寻求最小的整数 s, 使不定方程组

$$x_1^h + \cdots + x_s^h = y_1^h + \cdots + y_s^h, \quad 1 \leqslant h \leqslant k$$

有非无聊解, 也就是说, $x_1, \cdots, x_s$ 不是 $y_1, \cdots, y_s$ 的重新排列. 华罗庚[25] 指出: 估计 Prouhet 问题的解数是Виноградов 方法的主要环节; 另一方面, 这一方法也能用于 Prouhet 问题.

改进 $G(k)$ 上界的另一重要环节是寻求方程

$$x_1^k+\cdots+x_l^k=y_1^k+\cdots+y_l^k$$

的解数的上界, 此处 x 与 y 都是适合某些条件的整数.

Виноградов[27] 证明了 $G(k)\leqslant 3k\log k+11k$, 而 Davenport[28] 则对较小的 k 作出了重要的贡献. $k=3$ 时, 较好的估计 $G(3)\leqslant 7$ 则是属于Линник[28] 的. 运用Виноградов 强有力的方法, Dickson[30], Pillai[31] 与 Niven[32] 证明了: 当 $k\neq 4$ 与 $5, k>3$ 及 $\left(\frac{3}{2}\right)^k-\left[\left(\frac{3}{2}\right)^k\right]\leqslant 1-\left(\frac{1}{2}\right)^k\left\{\left(\frac{3}{2}\right)^k+3\right\}$ 时,每一整数都能表成 $g(k)=2^k+\left[\left(\frac{3}{2}\right)^k\right]-2$ 个非负整数的 k 次方之和. Siegel[33] 则将 Hardy-Littlewood 的圆法推广到代数数域上去.

Van der Corput[34] 给出了估计 Weyl 和的另一方法. 这一方法对圆内整点问题、除数问题与几何数论的其他问题, 以及 Riemann ζ- 函数论中的 Lindelöf 猜想, 都有着重要的作用. 以后, 他本人, Tichmarsh 与Виноградов 又推广与改进了这个方法.

关于 L- 函数及模函数论, 请读者参看百科全书中另一些专著"特殊的 Dirichlet 级数及其应用"与"解析数论中的模函数论". 同样, 本书亦不包括超越数论及 Diophantine 逼近论. 关于这些主题, 可以参看熟知的 Siegel, Гельфонд 与 Koksma 的书 (见后面的参考书籍).

Erdös 教授, Линник 教授与 Turán 教授都对本书提供了宝贵的意见, 作者仅向他们致以衷心地感谢. 在准备这本书的手稿时, 又得到了越民义先生与王元先生的帮助, 作者也借此机会向他们致以谢意.

第1章 初等方法

1.1 密　率

命 $\mathfrak{A}$ 表一由一些互不相同的非负整数 a 所成的集合. 命 $A(n)$ 表 $\mathfrak{A}$ 中不大于 n 之正整数的个数, 即 $A(n)=\sum\limits_{1\leqslant a\leqslant n}1$, 在此需要注意 0 并不计算在内. 若 $\alpha>0$ 为使 $A(n)\geqslant\alpha n$ 对于一切 $n\geqslant1$ 都成立的最大正数, 则称 $\mathfrak{A}$ 具有正密率 α. 显然 $\alpha\leqslant1$. 若 $\alpha=1$, 则 $\mathfrak{A}$ 包有全体自然数. 引入记号 $\mathfrak{B},b,B(n),\beta$ 及 $\mathfrak{C},c,C(n),\gamma$, 其间之关系一如 $\mathfrak{A},a,A(n),a$.

所有形如 $a+b(a\in\mathfrak{A},b\in\mathfrak{B})$ 的整数所成之集合 $\mathfrak{C}$, 称为 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的"和集", 记为 $\mathfrak{C}=\mathfrak{A}+\mathfrak{B}$. 关于 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的和集 $\mathfrak{C}$, Шнирельман[6]很简单地证明了下面两个重要定理:

(A) 若 $0\in\mathfrak{A}$, 则 $\gamma\geqslant a+\beta-a\beta$;

(B) 若 $0\in\mathfrak{A}$ 及 $a+\beta\geqslant1$, 则 $\gamma=1$, 即集合 $\mathfrak{C}$ 包有全体自然数.

命 $2\mathfrak{A}=\mathfrak{C}=\mathfrak{A}+\mathfrak{A}$, 并用归纳法定义 $s\mathfrak{A}=\mathfrak{A}+(s-1)\mathfrak{A}$, 则由 (A) 可知, $s\mathfrak{A}$ 的密率 $\geqslant1-(1-a)^s$. 命 $s_0=\left[\dfrac{\log2}{\log\dfrac{1}{1-\alpha}}\right]+1$, 则 $s_0\mathfrak{A}$ 的密率 $\geqslant\dfrac{1}{2}$. 又由 (B) 可知, 集合 $2s_0\mathfrak{A}$ 包有全体自然数, 故得:

(C) 若 $\mathfrak{A}$ 包有 0, 则每一正整数都可表成 $\mathfrak{A}$ 中 $2s_0$ 个元素之和.

Шнирельман给出了集合具有正密率的判别法:

(D) 命 $\mathfrak{A}^*$ 表一非负整数之集合, 其中的元素允许重复, 命 $\mathfrak{A}$ 为 $\mathfrak{A}^*$ 中不同元素所成之最大集合. 命 $r(\alpha)$ 表示 a 在 $\mathfrak{A}^*$ 中出现之次数, 若有 $a'>0$, 使对诸 $n\geqslant1$ 都有

$$\frac{1}{n}\left(\sum_{1\leqslant a\leqslant n}r(a)\right)^2\geqslant a'\left(\sum_{1\leqslant a\leqslant n}r^2(a)\right),$$

则 $\mathfrak{A}$ 有正密率 $a\geqslant a'$.

事实上, 由Буняковский-Schwarz 不等式可知

$$\left(\sum_{1\leqslant a\leqslant n}r(a)\right)^2\leqslant\sum_{1\leqslant a\leqslant n}r^2(a)\sum_{1\leqslant a\leqslant n}1=A(n)\sum_{1\leqslant a\leqslant n}r^2(a).$$

以上就是Шнирельман关于正整数集合的贡献的主要部分.

命 $\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_s$, 为密率都是 α 的 s 个集合. Хинчин[35]证明了：集合 $\mathfrak{A}_1 + \mathfrak{A}_2 + \cdots + \mathfrak{A}_s$ 的密率 $\geqslant \min(1, sa)$.

Mann[36] 在 1942 年证明了重要的猜想：$\gamma \geqslant \min(1, \alpha+\beta)$. 以后, Artin 与 Scherk[37] 又简化了 Mann 的证明. 请读者参考 Ostmann[38] 的书, 在那里详细地阐述了密率的理论及其应用.

1.2　Hilbert-Waring 定理

在讲Линник[39] 关于 Hilbert-Waring 定理的初等证明之前 (在此稍有简化与改进 [40]), 先证明下面两个引理.

引 1　命 $X, Y \geqslant 0$. 又命 $q(n)$ 为不定方程

$$x_1 y_1 + x_2 y_2 = n, \qquad |x_m| \leqslant X, \qquad |y_m| \leqslant Y, \qquad m = 1, 2, \tag{1}$$

的整数解数，则

$$q(n) \ll \begin{cases} (XY)^{\frac{3}{2}}, & 若 n = 0; \\ (XY)\displaystyle\sum_{d|n} \frac{1}{d}, & 若 n \neq 0. \end{cases} \tag{2}$$

当 $n = 0$ 时, 引理显然成立. 当 $n \neq 0$ 时, 只要证明在条件 $(x_1, x_2) = 1$ 及 $|x_2| \leqslant |x_1| \leqslant X$ 下, (1) 的解数 $q'(n) \ll XY$ 即可. 不失一般性, 可以假定 $X \leqslant Y$. 命 y_1', y_2' 是 (1) 的一组解答, 则其他解 y_1, y_2 可以表成 $y_1 = y_1' + tx_2, y_2 = y_2' - tx_1$. 因此 $|t| = \dfrac{|y_2' - y_2|}{|x_1|} \leqslant \dfrac{2Y}{|x_1|}$. 所以

$$q'(n) \leqslant \sum_{1 \leqslant |x_1| \leqslant X} \sum_{|x_2| \leqslant |x_1|} \frac{5Y}{|x_1|} \ll XY.$$

由引理立刻推出

$$\sum_{|a| \leqslant 2XY} q^2(a) \ll (XY)^3. \tag{3}$$

引 2　命 $k \geqslant 2$ 及

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x, a_k \ll 1, a_{k-1} \ll P, \cdots, a_1 \ll P^{k-1}$$

为一整系数多项式, 则

$$\int_0^1 \left| \sum_{x=0}^{P} \mathrm{e}^{2\pi \mathrm{i} f(x)\alpha} \right|^{8^{k-1}} \mathrm{d}\alpha \ll P^{8^{k-1}-k}, \tag{4}$$

此外与记号 $\ll$ 有关的常数仅依赖于 k.

仅仅是为了方便，我们才在这里使用了积分，我们可以毫无困难地把全部证明都用初等数论的语言写出来.

当 $k=2$ 时, (4) 之左端乃方程

$$f(x_1)+f(x_2)-f(y_1)-f(y_2)=f(x_3)+f(x_4)-f(y_3)-f(y_4),$$
$$x_m \ll P,\quad y_m \ll P,\quad m=1,2,3,4$$

的整数解数, 显然它不超过方程

$$z_1w_1+z_2w_3=z_3w_2+z_4w_4,\quad z_m\ll P,\quad w_m\ll P,\quad m=1,2,3,4$$

的整数解数. 由此, 由 (3) 可知, 引理当 $k=2$ 时是正确的. 现在用归纳法来证明引理. 由于

$$\left|\sum_{x=0}^{P}\mathrm{e}^{2\pi\mathrm{i}f(x)a}\right|^2=\sum_{x=0}^{P}\mathrm{e}^{-2\pi\mathrm{i}f(x)a}\sum_{-x\leqslant h\leqslant P-x}\mathrm{e}^{2\pi\mathrm{i}f(x+h)a}$$
$$=\sum_{|h|\leqslant P}{}'\sum_{x=1}^{p}{}'\mathrm{e}^{2\pi\mathrm{i}h\varphi(x,h)a},$$

此处 $\sum'$ 表示经过所示区间内整数的某一部分集合, 而

$$\varphi(x,h)=\begin{cases}\dfrac{1}{h}(f(x+h)-f(x)), & 若\ h\neq 0;\\ 0, & 若\ h=0,\end{cases}$$

故由 Hölder 不等式可知

$$\left|\sum_{x=0}^{P}\mathrm{e}^{2\pi\mathrm{i}f(x)a}\right|^{2\cdot 8^{k-2}}\ll P^{8^{k-2}-1}\sum_{|h|\ll P}{}'\left|\sum_{x=1}^{P}{}'\mathrm{e}^{2\pi\mathrm{i}h\varphi(x,h)a}\right|^{8^{k-2}}$$
$$=p^{8^{k-2}-1}\sum_{|h|\leqslant P}{}'\sum_{n}r(n)\mathrm{e}^{2\pi\mathrm{i}hna},\tag{5}$$

此处

$$r(n)=\int_0^1\left|\sum_{x=0}^{P}{}'\mathrm{e}^{2\pi\mathrm{i}\varphi(x,h)\beta}\right|^{8^{k-2}}\mathrm{e}^{-2\pi\mathrm{i}n\beta}\mathrm{d}\beta.\tag{6}$$

由归纳法假定可知 $r(n)\ll P^{8^{k-2}-(k-1)}$. 所以由 (3), 再将 (5) 式四方, 并从 0 至 1 求积分, 便得

$$\int_0^1\left|\sum_{x=0}^{P}\mathrm{e}^{2\pi\mathrm{i}f(x)a}\right|^{8^{k-1}}\mathrm{d}a$$

$$\begin{aligned}
&\ll P^{4(8^{k-2}-1)}\int_0^1\left|\sum_{|h|\leqslant P}{}'\sum_{n} r(n)\mathrm{e}^{2\pi\mathrm{i}hn\alpha}\right|^4\mathrm{d}\alpha\\
&\ll P^{4(8^{k-2}-1)}\sum_{hn+h'n'=h''n''+h'''n'''} r(n)r(n')r(n'')r(n''')\\
&\ll P^{4(8^{k-2}-1)+4(8^{k-2}-(k-1))+3(k-1+1)}\\
&=P^{8^{k-1}-k}.
\end{aligned}$$

取 $\mathfrak{A}_t^*$ 为整数

$$x_1^k+\cdots+x_t^k$$

所成之集合, 此处 x_m 各自经过全体非负整数. 定义 $\mathfrak{A}_t$ 为 $\mathfrak{A}_t^*$ 中的不同元素所成之最大子集. 命 $c_1=\dfrac{1}{2}8^{k-1}$ 及 $r(a)$ 为不定方程

$$x_1^k+\cdots+x_{c_1}^k=a,\quad x_m\geqslant 0$$

的解数, 则显然

$$\sum_{1\leqslant a\leqslant n} r(a)\gg\left(\frac{n}{c_1}\right)^{\frac{c_1}{k}}\gg n^{\frac{c_1}{k}}.$$

又由 (4) 可知

$$\sum_{1\leqslant a\leqslant n} r^2(a)\ll n^{\frac{2c_1}{k}-1},$$

故由定理 (D) 可知, 当 $k\geqslant 2$ 时, 集合 $\mathfrak{A}_{c_1}$ 有正密率, 因此我们证明了

Hilbert-Waring 定理 对于任意整数 $k\geqslant 2$, 互存在一仅依赖于 k 的整数 $s=s(k)$, 使每一正整数都是不超过 s 个正整数的 k 次方之和.

1.3 筛法及шнирельман- гольдбах 定理

Möbius 函数 $\mu(n)$ 是正整数 n 的函数, 其定义如下: $\mu(1)=1$; 若 n 能被一素数的平方所整除, 则 $\mu(n)=0$; 又若 n 为 r 个不同素数之乘积, 则 $\mu(n)=(-1)^r$.

古典的 Eratosthenes 筛法可以用下面的方式陈述出来; 命 P 为 $\leqslant\xi$ 的全体素数的乘积, 则

$$\sum_{d|(P,n)}\mu(d)=\begin{cases}1, & \text{若}n\text{无}\leqslant\xi\text{的素因子};\\ 0, & \text{其他情形}.\end{cases}\tag{7}$$

命 $\mathfrak{B}$ 为由 M 个相同或相异的整数 b 所成之集合, N_ξ 为 $\mathfrak{B}$ 中不能被 $\leqslant\xi$ 的素数整除的元素 b 的个数，则得

$$N_\xi=\sum_b\left(\sum_{d|(P,b)}\mu(d)\right).\tag{8}$$

交换 (8) 中的求和次序, 便得

$$N_\xi = \sum_{d|P} \mu(d) \sum_{d|b} 1 = \sum_{P|P} \mu(d) N(d), \tag{9}$$

此处 $N_d = \sum_{d|b} 1$ 为 $\mathfrak{B}$ 中能被 d 整除的元素 b 的个数.

用 Eratosthenes 原来的形式，可以将 (9) 式叙述为：先减掉集合 $\mathfrak{B}$ 中为 $2,3,5,\cdots$ (素数贯) 倍数的元素的个数，假如一个数为两个素数的乘积所整除，因为它被计算了两次，所以需要添上 $\mathfrak{B}$ 中为 $2\cdot 3,\ 2\cdot 5,\ 3\cdot 5,\ \cdots$ (两个素数乘积的贯) 的倍数的元素的个数. 又因为被三个素数的乘积整除的元素, 共计算了 $\binom{3}{1} - \binom{3}{2} = 0$ 次, 所以又需减掉 $\mathfrak{B}$ 中为 $2\cdot 3\cdot 5,\cdots$(三个素数乘积的贯) 整除的元素的个数, 如此等等.

若 $N(d)$ 有渐近表达式

$$N(d) = g(d)\frac{N}{d} + R_d, \tag{10}$$

此处 $g(d)$ 为无平方因子数的积性函数, 则由 (9) 得

$$\begin{aligned} N_\xi &= \sum_{d|P} \frac{\mu(d)}{d} g(d) N + O\Big(\sum_{d|P} | R_d |\Big) \\ &= N \prod_{p|P} \Big(1 - \frac{g(p)}{p}\Big) + O\Big(\sum_{d|P} | R_d |\Big). \end{aligned} \tag{11}$$

除了一些很显然的情况外, (11) 的余项常常比主项更大, 因此 (11) 几乎是无用的.

Brum[14] 对筛法作了重大的改进. 命

$$2 = p_1 < p_2 < \cdots < p_{k_0} \leqslant \xi$$

为 $\leqslant \xi$ 的全体素数, 又

$$k_0 \geqslant k_1 \geqslant \cdots \geqslant k_{t-1} \geqslant 1$$

为一整数集合. 命 Q 为具有如下形式的整数的集合:

$$d = 1, \quad d = p_{r_1} p_{r_2} \cdots p_{r_s}, \quad s \leqslant 2t, \tag{12}$$

其中 $r_1 > r_2 > \cdots > r_s$, $r_j \leqslant k_{[\frac{j-1}{2}]}, 1 \leqslant j \leqslant s$. 则得

$$\sum_{\substack{d|n \\ d\in Q}} \mu(d) \begin{cases} = 1, & 若n无 \leqslant \xi的素因子; \\ \geqslant 0, & 其他情形. \end{cases} \tag{13}$$

事实上, 若 n 无 $\leqslant \xi$ 的素因子, 则 (13) 式显然成立. 若 n 有 $\leqslant \xi$ 的素因子, 则以 p_0 表示 n 的最小素因子. 当 $d \in Q, d \mid n$ 及 d 的素因子个数为奇数时, 我们就定义 d_1 如下：若 $p_0 \mid d$, 则 $d_1 = \dfrac{d}{p_0}$; 若 $p_0 \nmid d$, 则 $d_1 = dp_0$. 因此 $d_1 \mid n, d_1 \in Q$ 且 d_1 的素因子个数为偶数. 由于每一个 d 都唯一地对应到一个 d_1, 故得 (13)

由 (13) 可知

$$\begin{aligned} N_\xi &\leqslant \sum_b \sum_{\substack{d \in Q \\ d \mid (b,P)}} \mu(d) = \sum_{d \in Q} \mu(d) \sum_{d \mid b} 1 \\ &= N \sum_{d \in Q} \mu(d) \frac{g(d)}{d} + O\Big(\sum_{d \in Q} \mid R_d \mid \Big). \end{aligned} \tag{14}$$

对于各种问题, 我们选取适当的 $k_0, \cdots, k_{t-1}$, 就能得到 N_ξ 的上界.

其次, 我们用另一集合 Q' 来代替集合 Q. 命 $k_0 \geqslant k_1 \geqslant \cdots \geqslant k_t \geqslant 1, Q'$ 为适合下面条件的整数集合：

$$d' = 1, \quad d' = p_{r_1} p_{r_2} \cdots p_{r_s}, \quad s \leqslant 2t+1,$$

其中 $r_1 > r_2 > \cdots > r_s$ 及 $r_i \leqslant k_{[\frac{1}{2}i]}$ 对应于 (13), 有

$$\sum_{\substack{d' \mid n \\ d' \in Q'}} \mu(d') \begin{cases} = 1, & \text{若}n\text{无} \leqslant \xi\text{的素因子;} \\ \leqslant 0, & \text{其他情形.} \end{cases}$$

类似地, 我们得到 N_ξ 的下界如下：

$$N_\xi \geqslant N \sum_{d' \in Q''} \frac{\mu(d') g(d')}{d'} + O\Big(\sum_{d' \in Q''} \mid R_{d'} \mid \Big). \tag{15}$$

取 $\mathfrak{B}$ 为整数

$$x(a-x), \quad 1 \leqslant x \leqslant a$$

的集合. 再适当地选取 (14) 中的 $k_i (1 \leqslant i \leqslant t-1)$. Шнирельман证明了下面的结果：命 $r(a)$ 为方程 $a = p_1 + p_2$ 的解数, 此处 p_1, p_2 为素数, 则

$$r(a) \ll \frac{a}{\log^2 a} \sum_{k \mid a} \frac{\mu^2(k)}{k}. \tag{16}$$

与 §1 相同的记号. 取 $\mathfrak{A}^*$ 为由整数 1 及诸整数 $a = p_1 + p_2 (1 < p_1, p_2 \leqslant a)$ 所成的集合，则显然有

$$\sum_{1 \leqslant a \leqslant n} r(a) = 1 + \sum_{p_1 + p_2 \leqslant n} 1 \geqslant \Big(\sum_{p_1 \leqslant \frac{n}{2}} 1 \Big)^2 \gg \Big(\frac{n}{\log n} \Big)^2.$$

又因 d 与 d' 的最小公倍数 $\{d_1, d_2\} \geqslant (dd')^{\frac{1}{2}}$, 故由 (16) 得到

$$\begin{aligned}\sum_{1\leqslant a\leqslant n} r^2(a) &\ll \sum_{4\leqslant a\leqslant n} \frac{a^2}{\log^4 a} \sum_{d|a} \frac{1}{d} \sum_{d'|a} \frac{1}{d'} \\ &\ll \frac{n^2}{\log^4 n} \sum_{d,d'\leqslant n} \frac{1}{dd'} \sum_{\substack{1\leqslant a\leqslant n \\ d|a, d'|a}} 1 \\ &\ll \frac{n^3}{\log^4 n}\left(\sum_{1\leqslant d\leqslant n} \frac{1}{d^{3/2}}\right)^2 \ll \frac{n^3}{\log^4 n}.\end{aligned}$$

于是由 §1, 定理 (D) 可知, 由 1 及可以表为两个素数之和的诸整数所成的集合具有正密率. 因此由定理 (C) 我们得到下面的享有盛名的定理.

Шнирельман-Гольдбах**定理**　存在整数 c, 使每一整数都是不超过 c 个素数之和.

命 s 表示最小的整数, 使每一充分大的整数都能表成不多于 s 个素数之和. Шнирельман的方法不仅证明了 s 的存在性, 而且可以得到 s 的明确上界. 他的方法给出 $s \leqslant 800,000$. Романов[41)] 又在以后证明了 $s \leqslant 2208$. 沿着这一方向, 还有如下更进一步的改进: Heilbronn, Landau 与 Scherk[42)] 得到 $s \leqslant 71$, 而估计 $s \leqslant 67$, 则是属于 Ricci[43)] 的.

在 (15) 中选取适当的 $k_0, k_1, \cdots$, Brun 首先证明了; 每一充分大的偶数都是两个各不超过 9 个素数的乘积之和. Rademacher[44)] 将 9 改进为 7, 而 Estermann[45)] 又将 7 减至 6.

Бухштаб[46)] 成功地以 4 代替了 6, 他改进这一结果的主要想法如下: 命

$$3 = p_1 < p_2 < \cdots < p_k$$

为不超过 y 的全体素数. 又命

$$(w) \qquad a;\ a_1,\ b_1;\ a_2,\ b_2;\ \cdots;\ a_k,\ b_k$$

为适合下面条件的整数集合:

$$a = 0\text{或}1, \quad a_i \neq b_i, \quad 0 \leqslant a_i, \quad b_i < p_i, \quad 1 \leqslant i \leqslant k;$$

而命 $F_w(x, y)$ 为适合下面条件的整数 n 的个数:

$$\begin{aligned}1 \leqslant n \leqslant x, \quad n \equiv a(\bmod 2), \quad n \not\equiv a_i(\bmod p_i),& \\ n \not\equiv b_i(\bmod p_i), \quad 1 \leqslant i \leqslant k,&\end{aligned}$$

则得

$$F_w(x; p_s) = F_w(x; p_{s-1}) - F_{w'_s}\left(\frac{x}{p_s}; p_{s-1}\right)$$

$$-F_{w_s''}\left(\frac{x}{p_s};p_{s-1}\right)+2\theta,\quad 0\leqslant|\theta|\leqslant 1. \tag{17}$$

命 $\nu > u \geqslant 2$. 将 $x^{\frac{1}{\nu}}$与$x^{\frac{1}{u}}$ 之间的素数依次排列为 $p_t \leqslant x^{\frac{1}{\nu}} < p_{t+1} < \cdots < p_k \leqslant x^{\frac{1}{u}} < p_{k+1}$, 则连续运用 (17) 便得

$$F_w(x;x^{\frac{1}{u}})=F_w(x;x^{\frac{1}{\nu}})-\sum_{i=t+1}^{k}F_{w_i'}\left(\frac{x}{p_i};p_{i-1}\right)$$
$$-\sum_{i=t+1}^{k}F_{w_i''}\left(\frac{x}{p_i};p_{i-1}\right)+2k\theta. \tag{18}$$

Бухштаб用 Brun 方法证明了：存在两个非负的阶梯函数 $\lambda(u)$及$\Lambda(u)$, 使当 x 充分大时, 下式对于 w 一致地成立：

$$\lambda(u)\frac{cx}{\log^2 x}\leqslant F_w(x;x^{\frac{1}{u}})\leqslant \Lambda(u)\frac{cx}{\log^2 x},\quad 15\geqslant u\geqslant 2. \tag{19}$$

由 (18), 我们可以构造两个阶梯函数

$$\lambda_1(u)\leqslant\lambda(\nu)-2\int_{u-1}^{\nu-1}\Lambda(z)\frac{z+1}{z^2}\mathrm{d}z$$

及

$$\Lambda_1(u)\geqslant\Lambda(\nu)-2\int_{u-1}^{\nu-1}\lambda(z)\frac{z+1}{z^2}\mathrm{d}z$$

它们分别具有与 $\lambda(u)$及$\Lambda(u)$ 相同的性质, 进而言之, 我们有

$$\lambda(u)\leqslant\lambda_1(u)\leqslant g(u)\leqslant\Lambda_1(u)\leqslant\Lambda(u).$$

不断运用这个原则, 并经过一些复杂的计算, 就能得到Бухштаб的结果

1.4　续

Selberg[15)17)47)] 对筛法作出了另一重要的改进.

命 $\lambda_1,\lambda_2\cdots$ 为一实数贯, 它满足 $\lambda_1=1$, 且当 $d>\sqrt{z}$ 时, $\lambda_d=0$. 则显然有

$$\left(\sum_{d|(n,P)}\lambda_d\right)^2\begin{cases}=1, & 若n无\leqslant\xi的素因子;\\ \geqslant 0, & 其他情形,\end{cases}$$

此处 $P=\prod\limits_{p\leqslant\xi}p$. 因此

$$N_\xi=\sum_b\left(\sum_{d|(b,P)}\mu(d)\right)\leqslant\sum_b\left(\sum_{d|(b,P)}\lambda_d\right)^2$$

$$= \sum_{\substack{d \leqslant \sqrt{z} \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{z} \\ d'|P}} \lambda_d \lambda_{d'} \sum_{\substack{b \\ \{d,d'\}|b}} 1$$

$$= N \sum_{\substack{d \leqslant \sqrt{z} \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{z} \\ d'|P}} \lambda_d \lambda_{d'} \frac{g(\{d,d'\})}{\{d,d'\}} + \sum_{\substack{d \leqslant \sqrt{z} \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{z} \\ d'|P}} \lambda_d \lambda_{d'} R_{\{d,d'\}},$$

此处 $\{d,d'\}$ 表示 d 与 d' 的最小公倍. Selberg 定出了使二次型

$$\sum_{\substack{d \leqslant \sqrt{z} \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{z} \\ d'|P}} \lambda_d \lambda_{d'} \frac{g(\{d,d'\})}{\{d,d'\}}$$

取极小值的诸 λ, 从而得到了 N_ξ 的上界.

为了估计 N_ξ 的下界，我们假定 $\lambda_1 = 1$. 若$p \leqslant \xi$,则$\lambda_p = 1$;若$d > \sqrt{\dfrac{z}{p}}$ 则 $\lambda_{d\cdot p} = 0$. 易知

$$1 - \sum_{p|(n,P)} \Bigg\{ \sum_{\substack{d|(n,P) \\ p'|d \Rightarrow p'<p}} \lambda_{d\cdot p} \Bigg\}^2 \begin{cases} = 1, & \text{若}n\text{无} \leqslant \xi\text{的素因子}; \\ \leqslant 0, & \text{其他情形}. \end{cases}$$

故得

$$N_\xi \geqslant \sum_b \Bigg(1 - \sum_{p|(b,P)} \Bigg\{ \sum_{\substack{d|(b,P) \\ p'|d \Rightarrow p'<p}} \lambda_{d\cdot p} \Bigg\}^2 \Bigg)$$

$$= N - \sum_{p \leqslant \xi} \sum_{\substack{d \leqslant \sqrt{\frac{z}{p}} \\ p'|d \Rightarrow p'<p \\ d|P}} \sum_{\substack{d \leqslant \sqrt{\frac{z}{p}} \\ p'|d' \Rightarrow p'<p \\ d'|P}} \lambda_{d\cdot p} \lambda_{d'\cdot p} \sum_{\substack{b \\ p\{d,d'\}|b}} 1$$

$$= N \Bigg(1 - \sum_{p \leqslant \xi} \frac{g(p)}{p} \sum_{\substack{d \leqslant \sqrt{\frac{z}{p}} \\ p'|d \Rightarrow p'<p \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{\frac{z}{p}} \\ p'|d' \Rightarrow p'<p \\ d'|P}} \lambda_{d\cdot p} \lambda_{d'\cdot p} \frac{g(\{d,d'\})}{\{d,d'\}} \Bigg)$$

$$- \sum_{p \leqslant \xi} \sum_{\substack{d \leqslant \sqrt{\frac{z}{p}} \\ p'|d \Rightarrow p'<p \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{\frac{z}{p}} \\ p'|d' \Rightarrow p'<p \\ d'|P}} \lambda_{d\cdot p} \lambda_{d'\cdot p} R_{p\cdot\{d,d'\}}$$

定出诸 λ, 使表达式

$$1 - \sum_{p \leqslant \xi} \frac{g(p)}{p} \sum_{\substack{d \leqslant \sqrt{\frac{z}{p}} \\ p'|d \Rightarrow p'<p \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{\frac{z}{p}} \\ p'|d' \Rightarrow p'<p \\ d'|P}} \lambda_{d\cdot p} \lambda_{d'\cdot p} R_{p\cdot\{d,d'\}}$$

取极大值. 我们便得到 N_ξ 的下界.

就已知的各种情况而言, Selberg 方法都比 Brun 方法精密. 例如, Shapiro 与 Warga[48] 用 Selberg 方法证明了: 每一充分大的自然数都是不超过 20 个素数之和. 尹文霖 [49] 在应用了渐近密率的两个结果之后, 证明了: 每一充分大的奇数都可表成不超过 17 个素数之和.

Eratosthenes-Brun-Selberg 筛法还可以用到许多其他问题上去. 我们现在列举一下这些问题的最近记录.

区间 $(A, A+N)$ 中的素数的个数 $\leqslant 2\dfrac{N}{\log N}+O\left(\dfrac{N}{\log^2 N}\log\log N\right)$, 此处与 O 有关的常数与 A 无关 (Selberg[47]).

不超过 N 的孪生素数对 $(p,p+2)(p<N)$ 的对数 $\leqslant 16\prod\limits_{p>2}\left(1-\dfrac{1}{(p-2)^2}\right)\dfrac{N}{\log^2 N}+O\left(\dfrac{N}{\log^3 N}\log\log N\right)$(Selberg[47]).

固定常数 $0<\delta<1$, 则在算术级数 $k_n+l(n=1,2,\cdots)$ 中不超过 x 的素数的个数

$$\leqslant \frac{2x}{\varphi(k)\log\dfrac{x}{k}}+O\left(\frac{x}{\log^2 x}\log\log x\right),$$

此处与 O 有关的常数对于适合 $k\leqslant x^{\delta}$ 的 k 都是一致的 (Чулановский[50]).

若 $F(x)$ 为无固定素因子的既约 k 次整值多项式, 则当$x=1,2,\cdots,N$ 时, 使 $F(x)$ 为素数的 x 的个数 $\leqslant 2e^{\gamma}\mu_F\dfrac{N}{\log N}+o\left(\dfrac{N}{\log N}\right)$, 此处 γ 为 Euler 常数, 而 μ_F 及与 o 有关的常数都是只依赖于 $F(x)$ 的常数 (王元 [51])

命 l 为适合不等式

$$\log\frac{5(6k-l)}{l+6}\leqslant 1.097(l+1)$$

的最小整数. Kuhn[52] 证明了: 存在无穷多个整数 x, 使 $F(x)$ 为不超过 $l+k$ 个素数的乘积.

关于以上问题的过去发展情况, 请参看 Ricci[43][53] 及 Heilbronn[54] 的文章.

王元 [55] 综合运用了Бухштаб方法与 Selberg 方法, 从而证明了每一充分大的偶数都是一个不超过 3 个素数的乘积及一个不超过 4 个素数的乘积之和. А.И.Виноградов[16]在运用了 Riemann ζ- 函数的某些性质之后, 证明了每一充分大的偶数都是两个素因子个数各不超过 3 的整数之和.

在广义 Riemann 猜想之下, 王元 [56] 证明了每一充分大的偶数都是一个素数及一个素因子个数不超过 4 的整数之和. 同样亦证明了存在无穷多个素数 p, 使 $p+2$ 为不超过 4 个素数的乘积.

1.5　素数定理的初等证明

是否可以不用复变函数论的理论来证明素数定理 [57], 这对于数学家来说, 是一个长期悬而未决的问题. 命 $\pi(x)$ 表示不超过 x 的素数的个数, 所谓素数定理, 就是

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\log x}}=1. \tag{20}$$

不久以前, Selberg[58] 与 Erdös[59] 才找到了一个适合上面要求的证明.

大家知道, 我们可以不用复变函数论的理论来证明下面这些结果:

a)

$$0<c_1<\frac{\pi(x)}{\frac{x}{\log x}}<c_2,\quad x\geqslant 2. \tag{21}$$

b) (20) 等价于

$$\lim_{x\to\infty}\frac{\theta(x)}{x}=1, \tag{22}$$

此处 $\theta(x)=\sum_{p\leqslant x}\log p$;

c)

$$\sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1).$$

以上都是Чебышев 的结果.

Selberg 证明的起点就是他的著名恒等式:

$$\theta(\xi)\log\xi+\sum_{p\leqslant\xi}\theta\left(\frac{\xi}{p}\right)\log p=2\xi\log\xi+O(\xi). \tag{23}$$

这是下面广义的 Möbius 反演公式的推论: 方程

$$G(x)=\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\log x \tag{24}$$

等价于

$$\sum_{n\leqslant x}\mu(n)G\left(\frac{x}{n}\right)=F(x)\log x+\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\Lambda(n), \tag{25}$$

此处当 n 为素数 p 的方幂时, $\Lambda(n)=\log p$, 否则 $\Lambda(n)=0$. 置 $F(x)=\sum_{n\leqslant x}\Lambda(n)-x+\gamma+1$($\gamma$ 为 Euler 常数), 则由 (24) 可知 $G(x)=O(\log^2 x)$. 故由 (25) 可得 (23)(Tatuzawa 与 Iseki[60]).

素数定理是 (23) 及下面这条与数论无关的定理的推论：

命 $K(x)$ 为非负递减函数,

$$g(x)=\int_o^x \mathrm{e}^u \mathrm{d}K(u). \tag{26}$$

若当 $x\to\infty$ 时, 有

$$0<c_1<g(x)\mathrm{e}^{-x}<c_2,\quad K(x)\sim x \tag{27}$$

及

$$g(x)+\frac{1}{x}\int_0^x g(x-u)\mathrm{d}g(u)\sim 2\mathrm{e}^x \tag{28}$$

则当 $x\to\infty$ 时,

$$g(x)\sim \mathrm{e}^x. \tag{29}$$

取 $K(u)=\sum\limits_{p\leqslant \mathrm{e}^u}\dfrac{\log p}{p}$,则$g(x)=\theta(\mathrm{e}^x)=\sum\limits_{p\leqslant \mathrm{e}^x}\log p$. 关系 (27) 就是Чебышев定理, 而结论 (29) 就是素数定理. 素数定理的证明虽然是初等的, 但却是十分复杂的.

Selberg 的初等方法还可以用来证明很多以往曾用解析方法得到的结果. 现在我们列举这些结果及其作者.

命 $\pi(x;q,l)$ 表示不超过 x 且 $\equiv l(\mathrm{mod}\ q)$ 的素数的个数. 若 $(q,l)=1$, 则

$$\pi(x;q,l)\backsim\frac{x}{\varphi(q)\log x}\quad (\text{Selberg}^{61)},\ \text{Shapiro}^{62)}).$$

每一个二次原型 $ax^2+2bxy+cy^2(a>0,D=b^2-ac$ 非平方数) 可以表出无穷多个素数 (Briggs[63)]).

命 K 为一代数数域, $N_{\mathfrak{p}}$ 表示素理想数 $\mathfrak{p}$ 的矩, 则

$$\pi_K(x)=\sum_{N_{\mathfrak{p}}\leqslant x}1\backsim\frac{x}{\log x}\quad (\text{Shapiro}^{64)}). \tag{30}$$

Forman 与 Shapiro[65)] 还证明了一个抽象素数定理, 不少素数定理都是它的特殊情形.

1.6　几何数论的初等方法

命 $A(x)$ 表示圆 $u^2+\nu^2\leqslant x$ 内整点 (u,ν) 的个数. Gauss 的“圆问题”就是去寻求最小的 ϑ, 使

$$A(x)=\pi x+O(x^{\vartheta+\varepsilon})$$

对所有的 $\varepsilon > 0$ 都成立. 类似地, 命 $D(x)$ 表示双曲线 $u\nu \leqslant x, u > 0, \nu > 0$ 内整点 (u, ν) 的个数. Dirichlet 的“除数问题”就是去录求最小的 ϑ, 使

$$D(x) = x \log x + (2\gamma - 1)x + O(x^{\vartheta+\varepsilon})$$

对所有的 $\varepsilon > 0$ 都成立, 此处 γ 为 Euler 常数. 迄今为止, 这两个问题都还没有解决. Gauss[66] 与 Dirichlet[67] 曾证明过 $\vartheta \leqslant \frac{1}{2}$. 这里我们将概述一下Виноградов[68]关于 $\vartheta \leqslant \frac{1}{3}$ 的初等 证明.

引　命 m 为整数, $A > 2, k \geqslant 1$,

$$S = \sum_{x=M}^{M+m-1} \{f(x)\},$$

此处 $f(x)$ 在区间 $M \leqslant x \leqslant M + m - 1$ 中定义, 它有二阶导数, 且适合

$$\frac{1}{A} \leqslant | f''(x) | \leqslant \frac{k}{A},$$

则

$$S - \frac{1}{2}m \ll (k^2 m \log A + kA)A^{-\frac{1}{3}}$$

证　命 $\tau = A^{\frac{1}{3}}$. 我们按照 $f'(x)$ 将求和区间分成若干子区间. 取 $M_1 = M$, 则有一对整数 (a_1, m_1) 满足

$$\left| f'(M_1) - \frac{a_1}{m_1} \right| \leqslant \frac{1}{m_1 \tau}, \quad 0 < m_1 \leqslant \tau,\ (a_1, m_1) = 1.$$

命 S_1 表示分和

$$S_1 = \sum_{x=M_1}^{M_1+m_1-1} \{f(x)\}.$$

其次, 置 $M_2 = M_1 + m_1$, 则有一对整数 (a_2, m_2) 满足

$$\left| f'(M_2) - \frac{a_2}{m_2} \right| \leqslant \frac{1}{m_2 \tau}, \quad 0 < m_2 \leqslant \tau,\ (a_2, m_2) = 1.$$

再命

$$S_2 = \sum_{x=M_2}^{M_2+m_2-1} \{f(x)\}.$$

进而言之, 取 $M_3 = M_2 + m_2$ 如此等等. 假定经过 s 步后得到

$$0 \leqslant M + m - 1 - M_{s+1} < \tau,$$

则得

$$| S - S_1 - \cdots - S_s | \leqslant \tau + 1.$$

引理的证明可以分成两步：第一, 估计每一分和, 得

$$\left| S_\nu - \frac{1}{2} m_\nu \right| \leqslant \frac{1}{2}(k+5).$$

第二, 证明步数 $s \ll \frac{km}{\tau} \log A + \frac{A}{\tau}$. 引理证完.

在圆问题上的应用.　显然

$$A(x) = 1 + 4[\sqrt{x}] + 8 \sum_{0<u\leqslant\sqrt{\frac{x}{2}}} [\sqrt{x-u^2}] - 4\left[\sqrt{\frac{1}{2}x}\right]^2.$$

命

$$\sum_{0<u\leqslant\sqrt{\frac{x}{2}}} [\sqrt{x-u^2}] = \sum_{0<u\leqslant\sqrt{\frac{x}{2}}} \sqrt{x-u^2} - \sum_{0<u\leqslant\sqrt{\frac{x}{2}}} \{\sqrt{x-u^2}\} = \sum\nolimits_1 - \sum\nolimits_2.$$

由 Euler 求和公式得到

$$\Sigma_1 = \frac{\pi}{8}x + \frac{x}{4} + \left(\frac{1}{2} - \left\{\sqrt{\frac{x}{2}}\right\}\right)\sqrt{\frac{x}{2}} - \frac{1}{2}\sqrt{x} + O(1).$$

又由引理可知

$$\Sigma_2 = \frac{1}{2}\sqrt{\frac{x}{2}} + O(x^{\frac{1}{3}}\log x),$$

因此

$$A(x) = \pi x + O(x^{\frac{1}{3}}\log x).$$

在除数问题上的应用.　显然

$$D(x) = \sum_{1\leqslant uv\leqslant x} 1 = 2\sum_{1\leqslant u\leqslant\sqrt{x}} \left[\frac{x}{u}\right] - [\sqrt{x}]^2.$$

由 Euler 求和公式可知

$$2\sum_{1\leqslant u\leqslant\sqrt{x}} \frac{x}{u} = x\log x + 2\left(\frac{1}{2} - \{\sqrt{x}\}\right)x^{\frac{1}{2}} + 2\gamma x + O(1).$$

命 t_0 为适合 $[\sqrt{x}]2^{-t_0} \geqslant 2x^{\frac{1}{3}} \geqslant [\sqrt{x}]2^{-t_0-1}$ 的整数, 则由引理可知

$$\sum_{1\leqslant u\leqslant\sqrt{x}} \left\{\frac{x}{u}\right\} = \sum_{t=0}^{t_0} \sum_{[\sqrt{x}]2^{-t-1}\leqslant u\leqslant[\sqrt{x}]2^{-t}} \left\{\frac{x}{u}\right\} + O(x^{\frac{1}{3}})$$

$$=\sum_{t=0}^{t_0}\left(\frac{1}{2^{t+2}}[\sqrt{x}]+O(x^{\frac{1}{3}}\log x)\right)+O(x^{\frac{1}{3}})$$
$$=\frac{1}{2}[\sqrt{x}]+O(x^{\frac{1}{3}}\log^2 x).$$

故得

$$D(x)=x\log x+(2\gamma-1)x+O(x^{\frac{1}{3}}\log^2 x)$$

附注. Jarnik[69] 推广了 Gauss 原来的方法, 从而证明了: 命 D 为一 Jordan 域, 其面积为 A, 而周长为 L, 则 D 中的整点个数 N 适合

$$|N-A|<L.$$

第 2 章　指数和的估计

2.1　Weyl 方法

Weyl 在他关于一致分布的开创性工作中, 首先引进了一个给予指数和以非无聊估计的方法. 这个方法基于不等式

$$\left|\sum_{x=a+1}^{a+P} \mathrm{e}^{2\pi\mathrm{i}\alpha x}\right| \leqslant \min\left(P, \frac{1}{|\sin \pi\alpha|}\right) \tag{31}$$

及下面的引理:

引　命 $k \geqslant 1$, 又命 $f(x)$ 为实函数及

$$\mathop{\Delta}_{y} Q(x) = \frac{1}{y}(Q(x+y) - Q(x)), \quad I = \sum_{x=1}^{p} \mathrm{e}^{2\pi\mathrm{i} f(x)}.$$

我们用记号 $\sum\limits_{x}^{P}$ 来表示在有限多个区间上的求和, 而这些区间的长度之和 $\ll P$. 于是当 $1 \leqslant \mu \leqslant k$ 时, 有

$$|\,1\,|^{2^{\mu}} \ll P^{2^{\mu}_{-\mu-1}} \sum_{y_1}^{P} \cdots \sum_{y_\mu}^{P} \sum_{x_{\mu+1}}^{P} \mathrm{e}^{2\pi\mathrm{i}(y_1\cdots y_\mu \mathop{\Delta}\limits_{y_\mu}\cdots \mathop{\Delta}\limits_{y_1} f(x_{\mu+1}))}, \tag{32}$$

此处与 $\ll$ 有关的常数仅依赖于 μ.

易知, 当 $\mu = 1$ 时引理成立. 由归纳法及Буняковский-Schwarz 不等式得到

$$|\,I\,|^{2^{\mu}} = |\,I^{2^{\mu-1}}\,|^2 \ll P^{2(2^{\mu-1}-\mu)} \left|\sum_{y_1}^{P} \cdots \sum_{y_{\mu-1}}^{P} \sum_{x_\mu}^{P} \mathrm{e}^{2\pi\mathrm{i}(y_1\cdots y_{\mu-1} \mathop{\Delta}\limits_{y_{\mu-1}} \mathop{\Delta}\limits_{y_1} f(x_\mu))}\right|^2$$

$$\ll P^{2^{\mu}-\mu-1} \sum_{y_1}^{P} \cdots \sum_{y_{\mu-1}}^{P} \left|\sum_{x_\mu}^{P} \mathrm{e}^{2\pi\mathrm{i}(y_1\cdots y_{\mu-1} \mathop{\Delta}\limits_{y_{\mu-1}} \cdots \mathop{\Delta}\limits_{y_1} f(x_\mu))}\right|^2,$$

故得 (32).

取 $f(x)$为$k(>1)$ 次多项式, $f(x) = \alpha x^k + \cdots$, 则由 (31) 及 (32)(取 $\mu = k-1$) 得

$$\left|\sum_{x=a+1}^{a+P} \mathrm{e}^{2\pi\mathrm{i} f(x)}\right|^{2k-1} \ll P^{2^{k-1}-1} + P^{2^{k-1}-k} \sum_{y_1}^{P} \cdots \sum_{y_{k-1}}^{P}{}^{*} \left|\sum_{x_k}^{P} \mathrm{e}^{2\pi\mathrm{i}k! y_1\cdots y_{k-1}\alpha x_k}\right|$$

$$\leqslant P^{2^{k-1}-1}+P^{2^{k-1}-k}\sum_{y_1,\cdots,y_{k-1}}^{P}{}^{*}\min\left(P,\frac{1}{\{k!y_1\cdots y_{k-1}\alpha\}}\right),\quad(33)$$

此处 * 表示条件 $y_1\cdots y_{k-1}\neq 0$, 而

$$\{\beta\}=\min(\beta-[\beta],[\beta]+1-\beta).$$

由除数函数的性质可知, 对于任意 $\varepsilon>0, Y=k!y_1\cdots y_{k-1}$ 的解答 $y_1,\cdots,y_{k-1}$ 的组数为 $O(Y^{\varepsilon})$. 所以

$$\left|\sum_{x=a+1}^{a+p}\mathrm{e}^{2\pi\mathrm{i}f(x)}\right|^{2^{k-1}}\ll P^{2^{k-1}-1}+P^{2^{k-1}-k+\varepsilon}\sum_{0<Y\ll P^{k-1}}\min\left(P,\frac{1}{\{Y\alpha\}}\right).\quad(34)$$

不等式 (34) 有着广泛的应用:

例 1 若 α 充分小, 例如 $\alpha=o(P^{-(k-1)})$, 则

$$\begin{aligned}\left|\sum_{x=a+1}^{a+P}\mathrm{e}^{2\pi\mathrm{i}f(x)}\right|^{2^{k-1}}&\ll P^{2^{k-1}-1}+P^{2^{k-1}-k+\varepsilon}\sum_{Y}\min\left(P,\frac{1}{\{Y\alpha\}}\right)\\&\ll P^{2^{k-1}-1}+P^{2^{k-1}-k+\varepsilon}\sum_{Y}\frac{1}{Y\mid\alpha\mid}\\&\ll P^{2^{k-1}-1}+P^{2^{k-1}-k+2\varepsilon}\frac{1}{\mid\alpha\mid},\end{aligned}$$

即对 $\varepsilon>0$,

$$\sum_{x=a+1}^{a+P}\mathrm{e}^{2\pi\mathrm{i}f(x)}\ll P^{1-2^{1-k}}+P^{1-k\cdot 2^{1-k}+\varepsilon}\mid\alpha\mid^{-2^{1-k}}.$$

例 2 若 $\alpha_k,\cdots,\alpha_0$ 皆为实数, 而且

$$f(x)=\alpha_kx^k+\cdots+\alpha_1x+\alpha_0,\quad\left|\alpha_k-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\ (h,q)=1,$$

则

$$\sum_{x=1}^{p}\mathrm{e}^{2\pi\mathrm{i}f(x)}\ll P^{1+\varepsilon}q^{\varepsilon}\left(\frac{1}{P}+\frac{1}{q}+\frac{q}{p^k}\right)^{2^{1-k}}.$$

证明依赖于下面的不等式:

$$\begin{aligned}\sum_{Y}^{P^{k-1}}\min\left(P,\frac{1}{\{Y\alpha_k\}}\right)&\ll\left(\frac{P^{k-1}}{q}+1\right)\max_{f}\left(\sum_{Y=f+1}^{f+q}\min\left(P,\frac{1}{\{Y\alpha_k\}}\right)\right)\\&\ll\left(\frac{P^{k-1}}{q}+1\right)(P+q\log q).\end{aligned}$$

2.2　Van der Corput 方法

如果分析一下上节的方法, 我们就会发现这个方法的两个重要步骤为: 1) 运用 $k-1$ 次Буняковский-Schwarz 不等式, 及 2) 直接处理 $k=1$ 的情形. 由于Буняковский-Schwarz 不等式用得愈多, 估计愈坏, 所以这就建议了这样一种做法: 1) 直接处理 $k=2$ 的情形, 及 2) 运用 $k-2$ 次Буняковский-Schwarz 不等式. 下面的 Hardy-Littlewood[70] 定理指出了这是可能的.

命 $\vartheta>0, \vartheta_1$ 为实数及 $A<B$, 则

$$\left|\sum_{x=A}^{B}{}' \mathrm{e}^{2\pi\mathrm{i}(\vartheta x^2+2\vartheta_1 x)}-\frac{\mathrm{e}^{\frac{\pi\mathrm{i}}{4}}}{\sqrt{\vartheta}}\sum_{x=A\vartheta+\vartheta_1}^{B\vartheta+\vartheta_1}\mathrm{e}^{\frac{-\pi\mathrm{i}}{\vartheta}(x-\vartheta_1)^2}\right|<\frac{1}{2}\left(1+\frac{1}{\sqrt{\vartheta}}\right), \tag{35}$$

此处 $\sum\limits_{x=A}^{B}{}'$ 表示项 $x=A$及$x=B$ 仅取其值之半.

由此可见,

$$\sum_{x=A}^{B}{}' \mathrm{e}^{2\pi\mathrm{i}(\frac{\vartheta}{2}x^2+\vartheta_1 x)} \ll (B-A)\mid\vartheta\mid^{\frac{1}{2}}+\mid\vartheta\mid^{-\frac{1}{2}}. \tag{36}$$

这由 van der Corput[34] 成功地将它变成下面的定理.

定理 1　若 $f(x)$ 为实函数, 它在区间 (a,b) 中有二阶导数, 并且适合

$$0<r<f''(x)\leqslant hr.\quad 或 0<r\leqslant -f''(x)\leqslant hr,$$

此处 $b\geqslant a+1$, 则

$$\sum_{a<n\leqslant b}\mathrm{e}^{2\pi\mathrm{i}f(n)}\ll h(b-a)r^{\frac{1}{2}}+r^{-\frac{1}{2}}.$$

下面的引理是一个与定理 1 类似的积分估计.

引 1　命 $f(x)$ 为实函数, 它在区间 (a,b) 中有二阶导数, 并且适合 $f''(x)\geqslant r>0$(或$f''(x)\leqslant -r<0$), 则

$$\left|\int_a^b \mathrm{e}^{2\pi\mathrm{i}f(x)}\mathrm{d}x\right|\leqslant\frac{8}{\sqrt{r}}.$$

下面的引理是沟通指数和与指数积分的桥梁.

引 2　命 $f(x)$ 为在区间 (a,b) 中有微商的实函数, 而 $f'(x)$ 为单调函数并且适合 $\mid f'(x)\mid\leqslant\theta<1$, 则

$$\sum_{a<n\leqslant b}\mathrm{e}^{2\pi\mathrm{i}f(x)}=\int_a^b \mathrm{e}^{2\pi\mathrm{i}f(x)}dx+O(1).$$

由第二中值定理, 立刻可以得到引 1. 又由 Euler 求和公式

$$\sum_{a<n\leqslant b} g(n)=\int_a^b g(x)\mathrm{d}x+\int_a^b\left(x-[x]-\frac{1}{2}\right)g'(x)\mathrm{d}x$$
$$+\left(a-[a]-\frac{1}{2}\right)g(a)-\left(b-[b]-\frac{1}{2}\right)g(b)$$

及 Fourier 展开

$$x-[x]-\frac{1}{2}=-\frac{1}{\pi}\sum_{n=1}^{\infty}\frac{\sin 2\pi nx}{n}$$

可以导出引 2.

现在由这两条引理来推导定理 1. 显然可以假定 $0<r<1$. 由于 $f'(x)$ 的单调性及 $|f'(b)-f'(a)|<(b-a)\cdot hr$, 所以可以将区间 (a,b) 分成 $\ll rh(b-a)$ 个子区间. 在每一子区间 (a',b')中, $|f'(b')-f'(a')|\leqslant\frac{1}{2}$. 故存在整数 ν, 使对任何 (a',b') 中的点 x, 都有 $|f'(x)-\nu|\leqslant\frac{3}{4}$. 由引 2 得到

$$\sum_{a'<x\leqslant b'}\mathrm{e}^{2\pi\mathrm{i}(f(x)-\nu x)}=\int_{a'}^{b'}\mathrm{e}^{2\pi\mathrm{i}(f(x)-\nu x)}\mathrm{d}x+O(1)$$

而由引 1 立刻得出定理 1.

关于步骤 1), van der Corput 引入下面的"基本不等式"来代替Буняковский-Schwarz 不等式: 命 $f(x)$ 为区间 $a+1\leqslant x\leqslant a+P$ 中的实函数, 则对适合 $2\leqslant\rho\leqslant P$ 的任何 ρ 整数都有

$$\left|\sum_{x=a+1}^{a+P}\mathrm{e}^{2\pi\mathrm{i}f(x)}\right|\leqslant\frac{\sqrt{2}P}{\sqrt{\rho}}+\left\{\frac{4P^2}{\rho}\sum_{\sigma=1}^{\rho-1}\left|\frac{1}{P-\sigma}\sum_{x=a+1}^{a+P-\sigma}\mathrm{e}^{2\pi\mathrm{i}(f(x+\sigma)-f(x))}\right|\right\}^{\frac{1}{2}}. \tag{37}$$

由定理 1 及基本不等式得

定理 2　命 $f(x)$ 为有连续 k 阶导数的实函数, 又命 $r\leqslant f^{(k)}(x)\leqslant hr$(或$r\leqslant -f^{(k)}(x)\leqslant hr$)及$b-a\geqslant 1$, 则

$$\sum_{a<n\leqslant b}\mathrm{e}^{2\pi\mathrm{i}f(n)}\ll h^{2^{2-k}}(b-a)r^{2^{\frac{1}{k-2}}}+(b-a)^{1-2^{2-k}}r^{-\frac{1}{2^{k}-2}},$$

此处与记号 $\ll$ 有关的常数与 k 无关.

另一个处理 $k=2$ 的方法, 基础于下面的可以用初等几何证明的定理: 命 $P\geqslant 1$ 及

$$0<\vartheta\leqslant f(2)-f(1)\leqslant f(3)-f(2)\leqslant\cdots\leqslant f(P)-f(P-1)\leqslant 1-\vartheta,$$

则

$$\left|\sum_{n=1}^{P} e^{2\pi i f(n)}\right| \leqslant \cot\frac{1}{2}\pi\vartheta \quad 或 < \frac{1}{\vartheta}.$$

关于不等式的证明, 请参看Кузьмин[71], Landau[72] 与 van der Corput[73] 的文章.

由这个不等式及归纳法 (即基本不等式) 得到

定理 3　命 $k \geqslant 2, f(x)$ 为在区间 $a+1 \leqslant x \leqslant a+P$ 中有 k 阶导数的实函数. 若对区间 $a+1 \leqslant x \leqslant a+P$ 中的全体 t 都有 $f^{(k)}(t) \geqslant r > 0$(或$f^{(k)}(t) \leqslant -r < 0$), 则

$$\left|\sum_{x=a+1}^{a+P} e^{2\pi i f(x)}\right| \ll P\left(\left(\frac{r}{R^2}\right)^{-\frac{1}{2^{k-2}}} + (rP^k)^{-\frac{1}{2^{k-1}}} + \left(\frac{rP}{R}\right)^{-\frac{1}{2^{k-1}}}\right), \tag{38}$$

此处 $R = \frac{1}{P}(f^{(k-1)}(a+p) - f^{(k-1)}(a+1))$.

定理 3 略佳于定理 1, 但在许多应用中, 定理 1 与定理 3 是等效的.

Van der Corput[74] 还将定理 1 进一步推广为

定理 4　命 $f(x)$ 为在区间 $a \leqslant x \leqslant b$ 中有三阶连续导数的实函数, 而 $f'(x)$ 为递减函数, 且

$$f'(a) = \alpha, \quad f'(b) = \beta.$$

又命

$$f'(x_\nu) = \nu, \quad a < \nu \leqslant \beta$$

及

$$2\pi r \leqslant | f''(x) | < Ar, \quad | f'''(x) | < AR,$$

则

$$\sum_{a<n\leqslant b} e^{2\pi i f(n)} = e^{-\frac{\pi i}{4}} \sum_{a<\nu\leqslant\beta} \frac{e^{2\pi i(f(x_\nu)-\nu x_\nu)}}{| f''(x_\nu) |^{\frac{1}{2}}} + O(r^{-\frac{1}{2}})$$
$$+ O(\log(2+(b-a)r)) + O((b-a)r^{\frac{1}{2}}R^{\frac{1}{5}}).$$

请参看Виноградов[75], Titchmarsh[76] 及 Phillips[77] 的文章. Titchmarsh[78] 将这方法推广到两个变数的情形, 这一推广的关键在于估计下面形状的二重指数积分

$$\int_a^b \int_\alpha^\beta e^{i f(x,y)} dx dy.$$

例如我们有

定理 5　命 $f(x,y)$ 为在矩形 $a \leqslant x \leqslant b, \alpha \leqslant y \leqslant \beta(b-a=l, \beta-\alpha=l)$ 中有三阶连续偏导数的实函数. 若在矩形中有

$$r \leqslant | f_{xx} | < Ar, \quad r \leqslant | f_{yy} | < Ar, \quad | f_{xy} | < Ar$$

与

$$| f_{xx}f_{yy} - f_{xy}^2 | \geqslant r^2,$$

则

$$\int_a^b \int_\alpha^\beta \mathrm{e}^{\mathrm{i}f(x,y)}\mathrm{d}x\mathrm{d}y = O\left(\frac{1+|\log l|+|\log r|}{r}\right).$$

闵嗣鹤[79] 对 Titchmarsh 定理给了一些改进.

2.3 виноградов 中值定理

无论以上所说的 Weyl 方法或 van der Corput 方法, 其主要之点都在于连续运用Буняковский-Schwarz 不等式; 而这个不等式用得愈多, 精密度就愈差. 1935 年, Виноградов[24][27][80] 创造了一个非常精深与强有力的方法, 以后他又多次改进自己的方法. 在这一节与下一节中将要谈到他的略经改进的最后结果 [81]. 华罗庚指出, Виноградов方法主要依赖于下面的中值定理.

定理 1　命 $f(x) = \alpha_k x^k + \cdots + \alpha_1 x$ 及

$$C_k = C_k(P) = \sum_{x=a+1}^{a+P} \mathrm{e}^{2\pi \mathrm{i} f(x)}.$$

又命 $t_1 = t_1(k) \geqslant \frac{1}{4}k(k+1) + lk$, 则

$$\int_0^1 \cdots \int_0^1 | C_k |^{2t_1} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \leqslant (7t_1)^{4t_1 l} P^{2t_1 - \frac{1}{2}k(k+1)+\delta} (\log P)^{2l},$$

此处 $\delta = \delta(k) = \frac{1}{2}k(k+1)\left(1-\frac{1}{k}\right)^l$.

由于这个定理的重要性, 所以我们给出较长的摘要.

引 1　一组整数 $(g_1, \cdots, g_b), 1 \leqslant g_\nu \leqslant H$, 假如它适合次之条件, 则谓之“佳位”组. 这个条件是: 其中至少有 k 个, 记为 $g_{j_1}, \cdots, g_{j_k}$, 适合

$$g_{j_{\nu+1}} - g_{j_\nu} > 1, \quad 1 \leqslant \nu \leqslant k-1. \tag{39}$$

非“佳位”组的个数最多是

$$b!\, 3^b H^{k-1}.$$

引 2　命 $C > 1, Q = RH, R > 1, H > 1$ 及

$$1 \leqslant g_1 < g_2 < \cdots < g_k \leqslant H, \quad g_\nu - g_{\nu-1} > 1,$$

此处 $g_1, \cdots, g_k$ 为整数, 又对于每一 $\nu(1 \leqslant \nu \leqslant k)$, 命 x_ν 在区间

$$-w+(g_\nu-1)R<x_\nu \leqslant -w+g_\nu R, \quad 0<w \leqslant Q$$

中变化, 则使

$$x_1^h+\cdots+x_k^h$$

分别落在长度不超过 $CQ^{(1-\frac{1}{k})h}(1 \leqslant h \leqslant k)$ 的区间中的整数组 $x_1, \cdots, x_k$ 的组数不超过

$$(2C)^k(2kH)^{\frac{1}{2}k(k-1)}Q^{\frac{1}{2}(k-1)}.$$

中值公式可以由归纳法及下面的定理推导出来.

定理 2　命 b 表一 $\geqslant \frac{1}{4}k(k+1)+k$ 的整数. 又命 η 为不超过

$$\frac{1}{k}\log Q/\log 2$$

的最大整数, 则

$$\int_0^1 \cdots \int_0^1 \mid C_k(Q) \mid^{2b} \mathrm{d}a_1 \cdots \mathrm{d}a_k$$
$$\leqslant (7b)^{4b}\max(1,\eta^2)Q^{2k-\frac{1}{2}(k+1)+\frac{2(b-k)}{k}} \int_0^1 \cdots \int_0^1 \left|C_k(Q^{1-\frac{1}{k}})\right|^{2(b-k)} \mathrm{d}a_1 \cdots \mathrm{d}a_k.$$

证明分成下面三步.

a) 不失一般性, 可以在 $C_k(Q)$ 中假定 $a=0$. 当$\eta<2$ 时, 定理显然成立. 因此, 我们假定 $\eta \geqslant 2$. 命 s 表一适合 $1 \leqslant s \leqslant \eta-1$ 的整数. 将 $C_k(Q)$ 分成 2^s 部分, 每份之长度 $R_s=Q^{2-s}$:

$$C_k(Q)=\sum_{g=1}^{2^s} \sum_{(g-1)R_s<x \leqslant gR_s} \mathrm{e}^{2\pi \mathrm{i} f(x)}=\sum_{g=1}^{2^s} Z_{sg}.$$

命 $Z=(C_k(Q))^b$, 则

$$Z=\sum^{2^{sb}} Z_{sg_1} \cdots Z_{sg_b},$$

此处 $\sum^{M}$ 表一和, 其项数最多是 M(在今后的证明中, 常有此种了解). 又简书

$$Z_s=Z_{s;g_1,\cdots,g_b}=Z_{sg_1} \cdots Z_{sg_b}.$$

如果 $g_1.\cdots,g_b$ 成一 “佳位” 组, 则 $Z_{s;g_1,\cdots,g_b}$ 称为 “佳位” 和, 而以 Z_s' 表之. 由引 1 可知, 非 “佳位” 和的个数不超过 $b!3^b2^{s(k-1)}$. 把非 “佳位” 和 Z_s 中的每一

因子分为二份. 如此从一个非"佳位"和 Z_s 得出 2^b 个和 Z_{s+1}. 故由全体非"佳位" Z_s 中所得的"佳位"的 Z_{s+1} 的个数显然不超过

$$M_s = b!3^b 2^{s(k-1)} \cdot 2^b = b!6^b 2^{s(k-1)}.$$

"佳位"的 Z_{s+1}用Z'_{s+1} 表之. 再如前法, 分割非"佳位"和 .　由于 Z_1 一定是非"佳位"的, 所以我们能够如此进行. 重复此项手续, 由 $s=1,2,\cdots,\eta-1$, 而用 Z'_η 表示由非"佳位"的 $Z_{\eta-1}$ 获得的全体 Z_η. 于是得到

$$Z = \sum_{s=1}^{\eta} \sum^{M_s} Z'_s.$$

b) 由Буняковский-Schwarz 不等式得出

$$|C_k(Q)|^{2b} = |Z|^2 \leqslant \eta \sum_{s=1}^{\eta} \left| \sum^{M_s} Z'_s \right|^2 \leqslant \eta \sum_{s=1}^{\eta} M_s \sum^{M_s} |Z'_s|^2. \tag{40}$$

不失一般性, 可以假定 $Z'_{s;g_1,\cdots,g_b} (1 \leqslant s \leqslant \eta-1)$ 中的 $g_1,\cdots,g_k$ 适合 (39). 把 $Z_{sg_i} (k+1 \leqslant i \leqslant b)$ 分成

$$\left[\frac{Q2^{-s}}{(Q^{1-\frac{1}{k}}-1)} \right] + 1 \leqslant Q^{\frac{1}{k}} \cdot 2^{1-s}$$

部分, 每一份的形式是

$$C^* = \sum_{w<x<w+Q'} \mathrm{e}^{2\pi \mathrm{i} f(x)},$$

此处 w 与 Q' 为适合

$$0 \leqslant w \leqslant g_i R_s \leqslant Q, \quad 0 < Q' \leqslant Q^{1-\frac{1}{k}}$$

的整数. 故由 Hölder 不等式可知

$$|Z_{sg_i}|^{2(b-k)} \leqslant \left(\sum^{Q^{\frac{1}{k}} 2^{1-s}} |C^*| \right)^{2(b-k)} \leqslant (Q^{\frac{1}{k}} 2^{1-s})^{2(b-k)-1} \sum^{Q^{\frac{1}{k}} 2^{1-s}} |C^*|^{2(b-k)}.$$

因为

$$|Z_{sg_{k+1}} \cdots Z_{sg_b}|^2 \leqslant \frac{1}{b-k} \sum_{i=k+1}^{b} |Z_{sg_i}|^{2(b-k)},$$

故由 (40) 得到

$$|Z|^2 \leqslant \frac{\eta}{b-k} \sum_{s=1}^{\eta} M_s (Q^{\frac{1}{k}} 2^{1-s})^{2(b-k)-1} \sum^{N_s} |Z_{sg_1} \cdots Z_{sg_k}|^2 |C^*|^{2(b-k)},$$

此处 $N_s = b!6^b 2^{s(k-1)}(b-k)Q^{\frac{1}{k}}2^{1-s}$. 因此

$$\int_0^1 \cdots \int_0^1 |Z|^2 \, \mathrm{d}a_1 \cdots \mathrm{d}a_k \leqslant \frac{\eta}{b-k}\sum_{s=1}^{\eta} M_s (Q^{\frac{1}{k}}2^{1-s})^{2(b-k)-1} \times \sum^{N_s} \int_0^1 \cdots \int_0^1 |Z_{sg_1} \cdots Z_{sg_k}|^2 |C^*|^{2(b-k)} \, \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k. \tag{41}$$

c) 积分

$$\int_0^1 \cdots \int_0^1 |Z_{sg_1} \cdots Z_{sg_k}|^2 |C^*|^{2(b-k)} \, \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k$$

等于下列不定方程组的解答数:

$$\begin{aligned} & x_1^h + \cdots + x_k^h + y_1^h + \cdots + y_{b-k}^h \\ = & x_1'^h + \cdots + x_k'^h + y_1'^h + \cdots + y_{(b-k)}'^h, \quad 1 \leqslant h \leqslant k, \end{aligned}$$

此处变数 y 与 y' 落在形如

$$w < y, y' \leqslant w + Q', \quad 0 < Q' \leqslant Q^{1-\frac{1}{k}}, \quad 0 \leqslant w \leqslant Q$$

的区间中, 而 x 与 x' 则在区间

$$(g_i - 1)R_s < x_i, \quad x_i' \leqslant g_i R_s$$

之中, $s \leqslant \eta - 1$, 为整数 $g_1, \cdots, g_k$ 适合条件 (39).

以 $X+w$及$Y+w$ 分别代替 x 及 y, 则 (41) 式也就是方程组

$$\begin{aligned} & X_1^h + \cdots + X_k^h + Y_1^h + \cdots + Y_{b-k}^h \\ = & X_1'^h + \cdots + X_k'^h + Y_1'^h + \cdots + Y_{b-k}'^h, \quad 1 \leqslant h \leqslant k \end{aligned}$$

的解数, 此处 Y' 在区间 $(0, Q')$ 之中, 而 X_i 及 X_i' 则在

$$-w + (g_i - 1)R_s < X_i, \quad X_i' \leqslant -w + g_i R_s, \quad 0 \leqslant w \leqslant Q$$

之中.

若先固定 X', 则 X 适合引 2 的要求, 其中 $R = R_s, C = 2(b-k)$及$H = 2^s$. 所以 X 及 X' 的组数不超过

$$\begin{aligned} & R_s^k \{4(b-k)\}^k (2k2^s)^{\frac{1}{2}k(k-1)} Q^{\frac{1}{2}(k-1)} \\ = & \{4(b-k)\}^k (2k)^{\frac{1}{2}k(k-1)} 2^{\frac{1}{2}sk(k-1)-sk} Q^{2k-\frac{1}{2}(k+1)}. \end{aligned}$$

又对已定的 X 及 X', Y 及 Y' 的组数不超过

$$\int_0^1 \cdots \int_0^1 \left| C_k(Q^{1-\frac{1}{k}}) \right|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k.$$

因此, 当 $1 \leqslant s \leqslant \eta - 1$ 时

$$\begin{aligned}&\int_0^1 \cdots \int_0^1 \mid Z_{sg_1} \cdots Z_{sg_k} \mid^2 \mid C^* \mid^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \\ \leqslant&\{4(b-k)\}^k (2k)^{\frac{1}{2}k(k-1)} 2^{\frac{1}{2}sk(k+1)-2sk} Q^{2_k - \frac{1}{2}(k+1)} \\ &\times \int_0^1 \cdots \int_0^1 \left| C_k(Q^{1-\frac{1}{k}}) \right|^{2(b-k)} \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k.\end{aligned}$$

当 $s = \eta$ 时, 由 η 的定义立刻得到这个不等式.

由 b), c) 即得定理.

关于较小的 k, 我们还有下面的结果.

定理 3　对于任何 $\varepsilon > 0$, 都有

$$\int_0^1 \cdots \int_0^1 \mid C_k(P) \mid^\lambda \mathrm{d}\alpha_1 \cdots \mathrm{d}\alpha_k \ll P^{\lambda - \frac{1}{2}k(k+1)+\varepsilon},$$

此处 λ 为 k 的函数, 它由下面的表来定义:

k	2	3	4	5	6	7	8	9	10[82]
λ	6	16	46	110	240	414	672	1080	1770

当 $k \geqslant 12$ 时, 对于

$$\lambda \leqslant 2k^2(3\log k + \log\log k + 4) - 4,$$

可以得到同样的结论 [23].

2.4　中值定理的推论

用仍然是Виноградов[27] 创造的 “由平均至单独” 的方法, 我们得到下面两个重要的推论.

定理 1　命 $k \geqslant 12, 2 \leqslant r \leqslant k$ 及

$$\left| \alpha_r - \frac{h}{q} \right| \leqslant \frac{1}{q^2}, \quad (h,q)=1,\ 1 \leqslant q \leqslant P^r.$$

又命

$$f(x) = \alpha_k x^k + \cdots + \alpha_1 x.$$

则当 $P \leqslant q \leqslant P^{r-1}$ 时,

$$S = \sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i} f(x)} \ll P^{1-\frac{1}{\sigma_k}+\varepsilon},$$

此处 $\sigma_k = 2k^2(2\log k + \log\log k + 3)$[23)83)].

定理 2　命 k 与 P 为整数; $k \geqslant 9, P \geqslant 2$. 又 $f(x)$ 为在区间 $(a+1, a+P)$ 中有 $(k+1)$ 阶连续导数的实函数. 又设在区间 $(a+1, a+P)$ 中有

$$1 \leqslant \lambda \leqslant \frac{f^{(k+1)}(x)}{(k+1)!} \leqslant 2\lambda$$

及

$$\lambda^{-\frac{1}{4}} \leqslant P \leqslant \lambda^{-1},$$

则

$$\sum_{x=a+1}^{a+P} \mathrm{e}^{2\pi \mathrm{i} f(x)} \leqslant \mathrm{e}^{32k\ \log^2 k} P^{1-\rho} \log P,$$

此处 $\rho = (56k^2 \log k)^{-1}$, 而与 $\ll$ 有关的常数为绝对常数 [27)84)85)].

这两个定理分别在 Waring 问题及素数分布问题上有着重要的应用. 现在我们将指出定理 1 证明的主要步骤. 用类似的想法可以证明定理 2.

对于 $0 < y \leqslant Y < P$,考虑

$$S_0 = \sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i}(f(x+y)-f(x))} = \sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i}\, \Phi(x)},$$

此处 $\Phi(x) = Y_{1x} + \cdots + Y_k x^k; Y_j = \begin{pmatrix} k \\ j \end{pmatrix} \alpha_k y^{k-j} + \cdots + \begin{pmatrix} j+1 \\ j \end{pmatrix} \alpha_{j+1} y + \alpha_j$, 易知 $| S_0 | - | S | \leqslant 2y$ 及

$$| S | \leqslant Y^{-1} \sum_{y=1}^{Y} | S_0 | + Y.$$

由 Hölder 不等式得到

$$| S |^{2t_1} \leqslant 2^{2t_1 - 1} \left(Y^{-1} \sum_{y=1}^{Y} | S_0 |^{2t_1} + Y^{2t_1}. \right)$$

命

$$S_1 = \sum_{x=1}^{p} \mathrm{e}^{2\pi \mathrm{i}(\beta_{1x} + \cdots + \beta_{k-1} x^{k-1} + \alpha_k x^k)}.$$

若 y 固定, 则 $Y_1, \cdots, Y_{k-1}$亦定. 命$\Omega(y)$ 表示适合

$$\{\beta_1 - Y_1\} \leqslant \frac{1}{2}P^{-2}Y, \cdots, \{\beta_{k-1} - Y_{k-1}\} \leqslant \frac{1}{2}P^{-k}Y, 0 \leqslant \beta_j \leqslant 1$$

的 $(\beta_1, \cdots, \beta_{k-1})$ 的区域. 若 $(\beta_1, \cdots, \beta_{k-1}) \in \Omega(y)$, 则

$$S_0 = S_1 + O(Y).$$

因此

$$|S|^{2t_1} \ll |S_1|^{2t_1} + Y^{2t_1}.$$

在区域 $\Omega(y)$ 上积分得

$$|S|^{2t_1} \ll P^{\frac{1}{2}k(k-1)+(k-1)}Y^{-(k-1)} \int \cdots \int_{\Omega(y)} |S_1|^{2t_1} \mathrm{d}\beta_1 \cdots \mathrm{d}\beta_{k-1} + Y^{2t_1}.$$

现在我们给定一点 $(\beta_1, \cdots, \beta_{k-1})$, 而来估计包含此点的区域 $\Omega(y)$ 的数目. 可以证明, $\Omega(y)$ 的个数不超过 $1 + \dfrac{Y}{q} + \dfrac{Yq}{P^r}$, 换言之, 单位立方体

$$0 \leqslant \beta_1 < 1, \quad \cdots, \quad 0 \leqslant \beta_{k-1} < 1$$

中的每一点最多被 $\ll \dfrac{Y}{q} + \dfrac{Yq}{P^r} + 1$ 个区域 $\Omega(y)$ 所遮盖. 因此

$$\begin{aligned}
|S|^{2t_1} &\ll P^{\frac{1}{2}k(k-1)+k-1}Y^{-k} \sum_{y=1}^{y} \int \cdots \int_{\Omega(y)} |S_1|^{2t_1} \mathrm{d}\beta_1 \cdots \mathrm{d}\beta_{k-1} + Y^{2t_1} \\
&\ll P^{\frac{1}{2}k(k-1)+k-1}Y^{-k} \left(\frac{Y}{q} + \frac{Yq}{P^r} + 1\right) \int_0^1 \cdots \int_0^1 |S_1|^{2t_1} \mathrm{d}\beta_1 \cdots \mathrm{d}\beta_{k-1} + Y^{2t_1}.
\end{aligned}$$

这个不等式是很重要的, 它是沟通“平均”与“单独”的桥梁. 由中值定理及一些计算即得定理 1.

2.5　群 的 特 征

命 $\mathfrak{G}$ 为一交换群. 若 $\chi(n)$ 为 $\mathfrak{G}$ 上定义的复函数, 且对 $\mathfrak{G}$ 中的全体元素 a, b, 都有 $\chi(a) \neq 0$及$\chi(ab) = \chi(a)\chi(b)$, 则称 $\chi(n)$ 为特征.

若对全体 $a \in \mathfrak{G}$ 都有 $\chi(a) = 1$, 则称此特征为主特征. 记之为 $\chi_0(a)$.

若 $\mathfrak{G}$ 有有限价 g, 则习知 $\mathfrak{G}$ 可以表成阶分别为 $g_1, \cdots, g_s$ 的巡迴群 $\mathfrak{G}_1, \cdots, \mathfrak{G}_s$ 的直乘积.　换言之,$\mathfrak{G}$ 的每一元素 a 可以唯一地表为 $a_1^{l_1} \cdots a_s^{l_s}$, 此处 $a_i \in \mathfrak{G}_i$ 及

$$o \leqslant l_i < g_i.$$

命 $\chi_u(a_i)=e^{2\pi iua_i/g_i}$ 为 $\mathfrak{G}_i$ 的一个特征, 则

$$\chi(a)=\chi_{u_1}(a_1^{l_1})\cdots\chi_{u_s}(a_s^{l_s})=\prod_{\nu=1}^{s}\mathrm{e}^{2\pi\mathrm{i}u_\nu l_\nu/g_\nu},\quad 0\leqslant u_\nu<g_\nu$$

为 $\mathfrak{G}$ 的一个特征. 因此我们得到 $\mathfrak{G}$ 的 $g_1\cdots g_s=g$ 个互不相同的特征. 易证, 这些就是群 $\mathfrak{G}$ 的全体特征. 由此可得下面两个基本关系式:

$$\sum_{a\epsilon\mathfrak{G}}\chi(a)\chi'(a)=\begin{cases}0, & 若\overline{\chi}\neq\chi';\\ g, & 若\overline{\chi}=\chi'\end{cases}\tag{42}$$

及

$$\sum_{\chi}\chi(a)\chi(b)=\begin{cases}0, & 若a\neq b^{-1};\\ g, & 若a=b^{-1}.\end{cases}\tag{43}$$

例 1　命 $\mathfrak{G}$ 为全体整数所成的加法群, 则对于每一实数 a, 可得一对整数 n 定义的特征

$$\chi(n)=\mathrm{e}^{2\pi\mathrm{i}an}.$$

例 2　命 $\mathfrak{G}$ 为 mod q 的剩余类的加法群, 则对每一整数 $a \bmod q$, 函数

$$\chi(n)=\mathrm{e}^{2\pi\mathrm{i}an/q}$$

为 $\mathfrak{G}$ 的一个特征. 这称为 $\bmod q$ 的加性特征.　易证, 这些就是 $\bmod q$ 的全体加性特征.

例 3　命 p 为一素数, 而 $\mathfrak{G}$ 为 $\bmod p$ 的缩剩余系所成的乘法群, 则对每一 a, 函数

$$\chi(n)=\mathrm{e}^{2\pi\mathrm{i}a\,\mathrm{ind}\,n/(p-1)}$$

为 $\mathfrak{G}$ 的一个特征. 同样可证, 这些就是 p 的全体乘性特征.

例 4　更一般些, 命 $\mathfrak{G}$ 为 $\bmod q$ 的缩剩余系所成的乘法群, $q=2^{l_{s+1}}p_1^{l_1}\cdots p_s^{l_s}$, 此处 $p_1,\cdots,p_s$ 为互不相同的奇素数. 当 $i=1,2,\cdots,s$ 时, 定义

$$\chi_i(n)=\chi_{u_i}(n)=\mathrm{e}^{2\pi\mathrm{i}u_i\mathrm{ind}\,n/\varphi(p_i^{l_i})},\quad 1\leqslant a_i\leqslant\varphi(p_i^{l_i}).$$

又当 $l_{s+1}\geqslant 2$ 时, 定义

$$\chi_{s+1}(n)=\begin{cases}(-1)^{\frac{1}{2}(n-1)a}, & a=1,2,\ 若l_{s+1}=2;\\ (-1)^{\frac{1}{2}(n-1)a}\mathrm{e}^{2\pi\mathrm{i}cb/2^{l-2}}, & a=1,2及1\leqslant c\leqslant 2^{l-2},\ 若l_{s+1}>2,\end{cases}$$

此处 b 为由 $n\equiv(-1)^{\frac{1}{2}(n-1)}5^b(\bmod 2^l)$, 及$b\geqslant 0$ 定义的整数, 则我们得到 $\bmod q$ 的全体特征

$$\chi(n)=\chi_{s+1}(n)\chi_1(n)\cdots\chi_s(n),\quad (n,q)=1.$$

为了方便起见, 当 $(n,q)>1$ 时, 常常定义

$$\chi(n)=0.$$

若 $\bmod q$ 的特征 $\chi(n)$ 满足下之条件, 即存在 q 的真因子 q' 使对适合 $n\equiv n'(\bmod q')$及$(n,q)=(n',q)=1$ 的全体 n 及 n' 都有 $\chi(n)=\chi(n')$, 则称 $\chi(n)$ 为非原特征. 否则, 称 $\chi(n)$ 为原特征.

2.6 特　征　和

常称首项为 1 的多项式为正则多项式. 命 $[q]$ 为含 q 个元素的域, $f(x)$为$[q]$ 上的 k 次既约多项式, $\chi(n)$为$[q]$ 的乘性特征. 常用 (f,g) 表示两个多项式 $f(x)$与$g(x)$ 的结式. 又对于任意 ν 次正则多项式 $g(x)$, 常置 $|g(x)|=q^{\nu}$. 定义

$$L(f,\chi,s)=\sum_{g}\frac{\chi(f,g)}{|g|^{s}},\tag{44}$$

此处的和号系对 $[q]$ 上的全体正则多项式求和. 显然

$$L(f,\chi,s)=\sum_{\nu=0}^{\infty}\frac{\sigma_{\nu}}{q^{\nu s}},\tag{45}$$

此处 $\sigma_{\nu}=\sum\limits_{g}\chi(f,g)$, 而其中的 g 通过全体 ν 次多项式. 因 $\chi(f,g)$ 与 $|g|$ 都是 g 的积性函数, 故得

$$L(f,\chi,s)=\prod_{G}\left(1-\frac{\chi(f,G)}{|G|^{s}}\right)^{-1},\tag{46}$$

此处的乘号系对 $[q]$ 上的全体正则既约多项式求积. 以下常假定 $\chi^{k}\neq\chi_{0}$.

定理 1　$L(f,\chi,s)$ 为 q^{-s} 的 $k-1$ 次多项式.

只要证明当 $\nu\geqslant k$ 时, $\sigma_{\nu}=0$ 即可. 命 ϑ 为 $f(x)=0$ 的一根, 并记, 由 $[q]$ 添加 ϑ 所成的域为 $[q^{k}]$, 则

$$(f,g)=(-1)^{k\nu}(g,f)=(-1)^{k\nu}Ng(\vartheta),$$

此处 $N(a)$ 表示 $[q^{k}]$ 中的元素关于 $[q]$ 的矩. 命 ψ 为 $[q^{k}]$ 上的延拓特征, 即

$$\psi(g(\vartheta))=\chi(-1)^{k\nu}\chi(f,g),$$

此处 ν 为 g 的次数. 记 $g(x)=x^{\nu}+a_{\nu-1}x^{\nu-1}+\cdots+a_{0}$, 则得

$$\sigma_{\nu}=\sum_{a_{0}\in[q]}\cdots\sum_{a_{\nu-1}\in[q]}\chi(f,g)=\varepsilon^{\nu}\sum_{a_{0}\in[q]}\cdots\sum_{a_{\nu-1}\in[q]}\psi(g(\vartheta)),$$

此处 $\varepsilon=\chi^k(-1)$. 当 $\nu\geqslant k$ 时, 固定 $a_k, \cdots, a_{\nu-1}$, 当 $a_0, \cdots, a_{k-1}$ 各自通过 $[q]$ 的全体元素时, $g(\vartheta)$ 通过域 $[q^k]$ 的全体元素. 因此当 $\nu\geqslant k$ 时,

$$\sigma_\nu=\varepsilon^\nu q^{\nu-k}\sum_{\xi\in[q^k]}\psi(\xi)=0.$$

定理 2　命

$$S(f,\chi)=\sum_{x\in[q]}\chi(f(x)),$$

则

$$S(f,\chi)=q^{s_1}+\cdots+q^{s_k-1}, \tag{47}$$

此处 $s_1, \cdots, s_{k-1}$ 表示 $L(f,\chi,s)$ 的零点.

在 (46) 式两端取对数, 便得

$$\log L(f,\ \chi,\ s)=\sum_G\sum_{\nu=1}^{\infty}\frac{1}{\nu}\chi(f,G^\nu)|G^\nu|^{-s}.$$

另一方面,

$$\log L(f,\ \chi,\ s)=-\sum_{h=1}^{\infty}\frac{1}{h}\Big(\sum_{i=1}^{h-1}q^{hs_i}\Big)q^{-hs}.$$

比较 q^{-s} 的系数, 得到

$$-\sum_{i=1}^{k-1}q^{s_i}=\sum_{|G^\nu|=q}\frac{1}{\nu}\chi(f,G^\nu)=\sum_{a\in[q]}\chi(f,x-a)=\sum_{a\in[q]}\chi(f(a)). \tag{48}$$

由 (48) 可知, 欲估计特征和 $\sum\limits_{a\in[q]}\chi(f(a))$, 只要估计 $q^{s_1}+\cdots+q^{s_{k-1}}$ 便已足够. 假如我们能够证明 $L(f,\chi,s)$ 的零点的实部都是 $\sigma=\dfrac{1}{2}$, 则得

$$\Big|\sum_{a\in[q]}\chi(f(a))\Big|\leqslant(k-1)\sqrt{q}.$$

关于这个问题 A. Weil 作出了重要的贡献. 命 Ω 为 $[q]$ 上的代数函数域, 定义 ζ- 函数

$$\zeta_\Omega(s)=\sum_{\mathfrak{A}}\frac{1}{|N(\mathfrak{A})|^s}=\prod_{\sigma}\Big(1-\frac{1}{|N(\sigma)|^s}\Big)^{-1},$$

此处 $\mathfrak{A}$ 经过 Ω 的全体整因子, 而 σ 则经过 Ω 的全体素因子, 又 $|N(\mathfrak{A})|$ 表示绝对矩. $\zeta_\Omega(s)$ 是一个具有周期 $2\pi i/\log q$ 的周期函数, 它在整个平面上, 除了在 $s\equiv0,1\bmod 2\pi i/\log q$ 处有一次极之外, 都是正则的.

定理 3(A. Weil)　$\zeta_\Omega(s)$ 的零点的实部都等于 $\frac{1}{2}$.

这个定理原来是 Artin 提出来的一个重要猜想. 对椭圆函数域的特殊情形, Hasse[86] 给予了证明. 而一般情形则由 A. Weil[87] 在 1948 年完全解决 (参看 Igusa[88] 与 Roquette[89] 的文章), 因为在 Weil 的证明中, 需要用到代数几何 [90] 的全部知识, 所以很难在此作一简单的概述.

Weil[91] 给出了定理 3 的另一推论.

定理 4　关于 Kloostermann 和, 我们有下面的估计:

$$\left|\sum_{x=1}^{p-1} \mathrm{e}^{2\pi \mathrm{i}(cx+\frac{d}{x})/p}\right| \leqslant 2\sqrt{p}. \tag{49}$$

Carlitz 与 Uchiyama[92] 还由定理 3 推出了下面的结果:

定理 5　命 $f(x)=a_kx^k+\cdots+a_1x+a_0, p\nmid a_k$, 则

$$\left|\sum_{x=1}^{p-1} \mathrm{e}^{2\pi \mathrm{i} f(x)/p}\right| \leqslant k\sqrt{p}. \tag{50}$$

关于 Kloostermann[93] 和的估计的历史如下: 在研究将整数表成 $ax^2+by^2+cz^2+dw^2$ 的形式的时候, Kloostermann 首先引入了这种类型的和, 所以通常就称之为 Kloostermann 和. 他得到的估计为 $O(p^{\frac{3}{4}})$. 以后Salié[94] 与 Davenport[95] 又将此估计改进为 $O(p^{\frac{2}{3}+\varepsilon})$.

关于 (50) 的估计的历史如下: Mordell[96] 证明它的阶为 $O(p^{1-\frac{1}{k}})$, 以后 Davenport[95] 又得到了估计 $O(p^{1-\frac{1}{m}})$, 此处 m 为形状如 2^g 与 $3\cdot 2^g$, 而又不超过 k 的整数中的最大者. 因为 Mordell 方法很有启发性, 所以我们在这里概要地叙述其证明过程: 表达式

$$\frac{1}{p^k}\sum_{a_k=1}^{p}\cdots\sum_{a_1=1}^{p}\left|\sum_{x=1}^{p} \mathrm{e}^{2\pi \mathrm{i}(a_kx^k+\cdots+a_1x)/p}\right|^{2k}$$

等于同余式组

$$\sum_{i=1}^{k} x_i^h \equiv \sum_{i=1}^{k} y_i^h (\bmod p), \quad 1\leqslant h\leqslant k, \quad 1\leqslant x, \quad y\leqslant p$$

的解数. 显然解数 $\leqslant k!\,p^k$. 进而言之, 他证明了, 对于固定的 $f(x)=a_kx^k+\cdots+a_1x$, $p\nmid a_k$, 存在 $\gg p^2$ 个不同的多项式 $f(\lambda x+\mu) \bmod p$ 使 $\left|\sum_{x=1}^{p} \mathrm{e}^{2\pi \mathrm{i} f(\lambda x+\mu)/p}\right|$ 等于 $\left|\sum_{x=1}^{p} \mathrm{e}^{2\pi \mathrm{i} f(x)/p}\right|$. 因此

$$\left|\sum_{x=1}^{p} \mathrm{e}^{2\pi \mathrm{i} f(x)/p}\right|^{2k} \ll p^{2k(1-\frac{1}{k})}.$$

故得定理.

华罗庚与闵嗣鹤[97] 将这一结果推广到两个变数的情形, 即

$$\sum_{x=1}^{p}\sum_{y=1}^{p} e^{2\pi i f(x,y)/p} \ll p^{2-\frac{2}{k}},$$

此处 $f(x,y)$ 为一 k 次多项式. 我们假定它不能化成一个变数的多项式, 用 Weil 方法, 希望可能得到某些改进.

2.7　完整三角和

命 q 表一 $\geqslant 1$ 的整数, $f(x)$ 为一整系数的 k 次多项式, 并且 $f(0)=0$, 即

$$f(x)=a_k x^k+\cdots+a_1 x.$$

我们现在研究指数和

$$S(q,f(x))=\sum_{x=1}^{q} e^{2\pi i f(x)/q}. \tag{51}$$

华罗庚[98] 在 1940 年证明了下面的结果:

定理 1　若 $(a_k,\ \cdots,\ a_1,\ q)=1$, 则

$$S(q,f(x)) \ll q^{1-\frac{1}{k}+\varepsilon},$$

此处 ε 为一任给的正数, 而与 $\ll$ 有关的常数仅依赖于 k 与 ε.

证　当 $(q_1,q_2)=1$ 时,

$$S(q_1q_2,\ f(x))=S(q_1,\ f(q_2x)/q_2)S(q_2,\ f(q_1x)/q_1).$$

因此, 欲计算 (或估计)(51), 只要计算当 $q=p^l$ 时的情况便已足够, 此处 p 为素数. 当 $l=1$ 时, 此即 § 12 中证明的定理. 现在对 l 用归纳法.

由 $p^t \,\|\, (ka_k,\ \cdots,\ a_1)$ 来定义 t, 当 $l<2(t+1)$ 时, 定理显然成立. 当 $l\geqslant 2(t+1)$ 时, 置

$$S(p^l,\ f(x))=\sum_{\nu=1}^{p}\ \sum_{\substack{0\leqslant x<p^l\\ x\equiv \nu(\mathrm{mod}\ p)}} e^{2\pi i f(x)/p^l}=\sum_{\nu=1}^{p} S_\nu.$$

若 ν 非同余式 $f'(x)\equiv 0(\mathrm{mod}\ p^{t+1})(0\leqslant x<p)$ 的解, 则得 $S_\nu=0$. 若 ν 为同余式 $f'(x)\equiv 0(\mathrm{mod}\ p^{t+1})(0\leqslant x<p)$ 的解, 则易见能整除 $f(\nu+py)-f(\nu)$ 全体系数的 p 的最高方幂 p^{σ_ν} 适合 $p\leqslant p^{\sigma_\nu}\leqslant p^k$. 因此

$$|S_\nu| = \left|\sum_{y=0}^{p^l-1} \mathrm{e}^{2\pi\mathrm{i} f(\nu+py)/p^l}\right| \leqslant p^{\sigma_\nu(1-\frac{1}{k})}|S(p^{1-\sigma_\nu},\ g_\nu(x))|,$$

此处 $g_\nu(x) = p^{-\sigma_\nu}(f(\nu+px)-f(\nu))$. 若能整除 $g_\nu'(x)$ 全体系数的 p 的最高方幂为 p^u, 则易证同余式 $g_\nu'(x) \equiv 0(\bmod\ p^{u+1})$ 的解数不超过同余式 $f'(x) \equiv 0(\bmod\ p^{t+1})(0 \leqslant x < p)$ 的根 ν 的重数. 故由归纳法即得定理.

同法, 我们可以证明, 若 $p^{-t}f'(x) \equiv 0(\bmod\ p)$ 的根的重数 $\leqslant m$, 则

$$S(f(x), p^l) = O(p^{l(1-\frac{1}{m+1})}).$$

华罗庚 [99] 还将他的定理推广到有理数域上的任何 n 次代数数域上去.

2.8　不完整和的估计方法

命 $g(x)$ 为有周期 q 的函数, 对于 $0 \leqslant x < q$ 显然有

$$\begin{aligned} g(x) &= \frac{m}{q} + \frac{1}{q}\sum_{n=1}^{q-1} \mathrm{e}^{2\pi\mathrm{i}n\frac{x}{q}}(1-\mathrm{e}^{-2\pi\mathrm{i}m\frac{n}{q}})/(1-\mathrm{e}^{-2\pi\mathrm{i}\frac{n}{q}}) \\ &= \begin{cases} 1, & 若\ 0 \leqslant x < m; \\ 0, & 若\ m \leqslant x < q. \end{cases} \end{aligned}$$

因此

$$\begin{aligned} \sum_{x=0}^{m-1} f(x) &= \sum_{x=0}^{q-1} f(x)g(x) \\ &= \frac{m}{q}\sum_{x=0}^{q-1} f(x) + \frac{1}{q}\sum_{x=0}^{q-1} f(x)\sum_{n=1}^{q-1} \mathrm{e}^{2\pi\mathrm{i}n\frac{x}{q}}(1-\mathrm{e}^{-2\pi\mathrm{i}m\frac{n}{q}})/(1-\mathrm{e}^{-2\pi\mathrm{i}\frac{n}{q}}). \end{aligned}$$

故得

$$\left|\sum_{x=0}^{m-1} f(x) - \frac{m}{q}\sum_{x=0}^{q-1} f(x)\right| \leqslant \sum_{n=1}^{q} \frac{1}{n}\left|\sum_{x=0}^{q-1} f(x)\mathrm{e}^{2\pi\mathrm{i}\frac{nx}{q}}\right|. \tag{52}$$

由此可以将不完整和的估计归结为完整和的估计. 例如 [100], 当 $1 \leqslant m \leqslant q$ 时,

$$\sum_{x=1}^{m} \mathrm{e}^{2\pi\mathrm{i}\frac{f(x)}{q}} \ll q^{1-\frac{1}{k}+\varepsilon}d^{\frac{1}{k}}, \tag{53}$$

此处 $(a_k,\ \cdots,\ a_2,\ q) = d$, 而与 $\ll$ 有关的常数仅依赖于 ε 及 k.

类似地, 若

$$\left|a-\frac{h}{q}\right| \leqslant \frac{1}{qP^{k-1}},$$

则由部分求和得到

$$\sum_{x=1}^{P} \mathrm{e}^{2\pi \mathrm{i} f(x) a} \ll P q^{-\frac{1}{k}+\varepsilon}. \tag{54}$$

命 $p>2$ 为素数, $(a,p)=1$. 若 $x^n \equiv a(\bmod p)$ 有解, 则称 a 为 $\bmod p$ 的 n 次剩余, 否则称 a 为非剩余.

命 χ 为 $\bmod p$ 之原特征. 特征和 $S(m)=\sum\limits_{n \leqslant m} \chi(n)$ 的估计在解析数论中有着重要意义. 例如Линник 与 Rényi[101] 证明了: 命 $N_{\min}^{*}$, 表示使 $\chi(n) \neq 1$ 成立的绝对值最小 $(\neq 0)$ 的整数 n, 则或者当 $p>p_0(\varepsilon)$ 时, $N_{\min}^{*}<p^{\varepsilon}$, 或者 $|S(m)| \ll \sqrt{p}$.

下面是习知的 Pólya[102] 的结果: 对于所有的特征 $\chi \neq \chi_0 \bmod p$, 都有

$$|S(m)|<\sqrt{p} \log p.$$

由此立刻可知, 最小正二次非剩余 $N_{\min}<\sqrt{p} \log p$.

关于 $N_{\min}$ 的上界的估计, 至今最好的结果还是属于Виноградов[103] 的. 他得到如下的结果:

定理　若 n 为 $p-1$ 的异于 1 的因子, 则对于全体充分大的 p, $\bmod p$ 的最小 n 次非剩余

$$\leqslant p^{\frac{1}{2k}}(\log p)^2, \quad k=\mathrm{e}^{\frac{n-1}{n}}.$$

特别由此得出 $N_{\min} \leqslant T=p^{\frac{1}{2\sqrt{\mathrm{e}}}}(\log p)^2$.

这个结果的证明是很简易的. 事实上, 若区间 $[1,\ T]$ 中的全体整数都是二次剩余, 则不超过 $Q=\sqrt{p} \log^2 p$ 的二次非剩余都有一素因子 q 适合 $T<q \leqslant Q$. 因此, 不超过 Q 的二次非剩余的个数 N 适合

$$N \leqslant \sum_{T<q \leqslant Q}\left[\frac{Q}{q}\right]<Q \sum_{T<q \leqslant Q} \frac{1}{q}.$$

不难证明

$$\sum_{T<p \leqslant Q} \frac{1}{p}=\log \frac{\log Q}{\log T}+O\left(\frac{1}{\log Q}\right).$$

因此, 由上面的不等式及习知的结果

$$N=\frac{1}{2} Q+\frac{\theta}{2} \sqrt{p} \log p, \quad |\theta| \leqslant 1$$

即得定理.

在广义 Riemann 猜想之下, Ankeny[104] 证明了：

$$N_{\min} \ll (\log p)^2.$$

由 Pólya 定理及下面习知的等式：

$$\sum_{k|p-1} \frac{\mu(k)}{\varphi(k)} \sum_{\chi^{(k)}} \sum_{n=1}^{g(p)-1} \chi^{(k)}(n) = 0, \tag{55}$$

此处 $g(p)$ 表示 p 的最小正原根, 而 $\chi^{(k)}$ 通过 mod k 的全体 $\varphi(k)$ 个特征. Виноградов[105] 证明了

$$g(p) = O(2^m \sqrt{p} \log \log p),$$

此处 m 表示 $p-1$ 的不同的素因子个数.

华罗庚用

$$\sum_{k|p-1} \frac{\mu(k)}{\varphi(k)} \sum_{\chi^{(k)}} \sum_{a=0}^{|h(p)|-1} \sum_{n=-a}^{a} \chi^{(k)}(n) = 0$$

代替 (55), 此处 $h(p)$ 表示 p 的有最小绝对值的原根; 同时证明：对于全体非主特征 $\chi(n)$, 都有

$$\frac{1}{A+1} \left| \sum_{a=0}^{A} \sum_{n=-a}^{a} \chi(n) \right| \leqslant \sqrt{p} - \frac{A+1}{\sqrt{p}}, \quad 1 \leqslant A < p, \tag{56}$$

由此他 [106] 得到了

$$|h(p)| < 2^m \sqrt{p}$$

及

$$g(p) < 2^{m+1} \sqrt{p}.$$

Erdös[107] 用 Brun 方法证明了：对于充分大的 p, 有

$$g(p) < p^{\frac{1}{2}} \log^{17} p.$$

在广义 Riemann 猜想下, Ankeny[104] 证明了：

$$g(p) = O(2^m \log^2 p \log^2(2^m \log p)).$$

关于 $g(p)$ 的下界的估计, Turan[108] 证明了：

$$g(p) = \Omega(\log p).$$

华罗庚[109] 还用 (56) 证明了:

$$\log \varepsilon < \sqrt{d}\Big(\frac{1}{2}\log d + 1\Big),$$

此处 $\varepsilon = (x_0 + \sqrt{d}\, y_0)/2$; x_0, y_0 为 Pell 方程 $x^2 - dy^2 = 4$ 的最小正解, 而 d 为 $\equiv 0$ 或 1(mod 4) 的非平方正整数.

这个结果是下面 Schur[110] 定理的改进:

$$\log \varepsilon < \sqrt{d}\Big(\frac{1}{2}\log d + \frac{1}{2}\log\log d + 1\Big).$$

在所有上面说到的关于 $N_{\min}, g(p)$ 与 $\log \varepsilon$ 的定理的证明中, 都会用到

$$\tau(\chi) = \sum_{n=1}^{p} \chi(n) e^{2\pi i \frac{n}{p}}.$$

不难证明, 对于 mod p 的原特征, 有

$$|\tau(\chi)| = \sqrt{p}.$$

而对于 mod p 的实原特征, 则有确切的数值:

$$\tau(\chi) = \begin{cases} \sqrt{p}, & 若\chi(-1) = 1; \\ i\sqrt{p}, & 若\chi(-1) = -1. \end{cases}$$

关于素数为变数的特征和, Линник[111] 得到下面的定理:

定理 1　a) 对于 mod q 的复特征 $\chi(n)$, 有

$$\sum_{p \leqslant N} \chi(p) \ll \frac{N}{\log N}\Big\{\exp\Big(-c_0\frac{\log N}{\log q}\Big) + \frac{1}{\log q}\Big\}.$$

b) 命 $-q < 0$ 为基本判别式, 则

$$\sum_{p \leqslant N} \Big(\frac{-q}{p}\Big) \ll \frac{N}{\log N}\Big\{\exp\Big(-c_0\frac{\log N}{\log q}\Big) + \exp\Big(-c_0\frac{h(-q)}{\sqrt{q}}\log N\Big) + \frac{1}{\log q}\Big\},$$

此处 $h(-q)$ 为 $k(\sqrt{-q})$ 的类数, 而 c_0 为一绝对常数.

Линник 这个结果的证明主要依赖于下面的引理.

引　命 $\chi(n)$ 为 mod q 的一个实的或复的特征, $L(s,\chi)$ 为与它对应的 L- 函数, 则存在绝对常数 c, 使当 $q \to \infty$ 时, $L(s,\chi)$ 在临界区域中的零点 $\rho_k = \beta_k + i_{t_k}$ 适合

$$\sum_{\rho_k} \frac{m_k}{|\rho_k|^2}\exp(-c\sigma_k \log q) \ll 1,$$

此处 m_k 为零点 ρ_k 的重数, 而 $\sigma_k = 1 - \rho_k$.

Paley[112] 证明了：存在正常数 A, 两个正整数贯 (n_ν) 与 (q_ν) 及原特征贯 $\chi_\nu \bmod q_\nu$, 使

$$\left|\sum_{m=1}^{n_\nu} \chi_\nu(m)\right| \geqslant A\sqrt{q_\nu} \log\log q_\nu, \quad \nu = 1,\ 2,\ \cdots.$$

以后, Chowla[113] 又在同样的假定下证明了

$$\sum_{m=1}^{n_\nu} \chi_\nu(m) \geqslant A\sqrt{q_\nu} \log\log q_\nu.$$

Batman, Chowla 与 Erdös[114] 在 1950 年得到了同样类型的结果, 但其中 q 限制为素数. 这一结果, 以往 Chowla[115] 会在广义 Riemann 猜想下得到过. 因为在百科全书中, 还有关于特殊 Dirichlet 级数及其应用的专著, 所以这类结果就不在此详细阐述了.

2.9　素数变数的指数和

我们现在来介绍Виноградов[10)27] 关于估计素数变数的指数和的开创性方法. 他是首先给出这种和以非无聊估计的人. 依靠这个估计, 他证明了著名的“三素数定理”. 这种和的形状为

$$\sum_{p \leqslant N} \mathrm{e}^{2\pi i f(p)},$$

此处 p 通过不超过 N 的全体素数. 首先, 我们要指出在Виноградов 工作中经常用到的一个重要原则; 他常常将他研究的问题归结为下面形状的二重指数和的估计：

$$\sum \mathrm{e}^{2\pi i auv},$$

此处 u 与 v 分别通过某个整数集合. 在用这个方法时, u 与 v 常常是大量其他变量的函数. 一般言之, 当 u 与 v 的分布有一定程度的规则时, 我们就可能对上面的和进行估计. 将这个原则应用到所研究的问题时, 依赖于下面的引理.

引　假定我们有三个由正整数组成的递增贯; u 取全体 $u_1\ u_2$, 此处 u_1 经过第一贯中的全体整数, u_2 独立地经过第二贯中的全体整数, 而 v 则经过第三个整数贯, 又假定

$$1 < U < N, \quad U < U' \ll U, \quad a = \frac{h}{q} + \frac{\theta}{q^2}, \quad (h, q) = 1, \quad 1 < q < N$$

及

$$S=\sum_{U<u\leqslant U'}\sum_{v\leqslant \frac{N}{u}}\mathrm{e}^{2\pi\mathrm{i}auv},$$

则

$$S\ll L^2N(q^{-1}+qN^{-1}+U^{-1}+UN^{-1})^{\frac{1}{2}},$$

此处 $L=\log N$.

证　命 $\xi(z)$ 为 $z=u_1u_2$ 的解数, 则

$$S=\sum_{U<z\leqslant U'}\xi(z)\sum_{\nu\leqslant \frac{N}{Z}}\mathrm{e}^{2\pi\mathrm{i}azv},$$

此处 z 经过所示区间中的全体整数. 于是由Буняковский-Schwarz 不等式得到

$$\begin{aligned}
S^2\ll&\sum_{U<z\leqslant U'}\xi^2(z)\sum_{U<z\leqslant U'}\left|\sum_{v\leqslant \frac{N}{z}}\mathrm{e}^{2\pi\mathrm{i}azv}\right|^2\\
\ll&UL^3\sum_{U<z\leqslant U'}\sum_{v\leqslant \frac{N}{Z}}\sum_{v'\leqslant \frac{N}{z}}\mathrm{e}^{2\pi\mathrm{i}az(v-v')}\\
=&UL^3\sum_{v\leqslant \frac{N}{z}}\sum_{v'\leqslant \frac{N}{z}}\sum_{U<z<\min(\frac{N}{v},\ \frac{N}{v'},\ U')}\mathrm{e}^{2\pi\mathrm{i}az(v-v')}\\
\ll&UL^3\sum_{v\leqslant \frac{N}{z}}\sum_{v'\leqslant \frac{N}{z}}\min\left(U,\frac{1}{\{\alpha(v-v')\}}\right).
\end{aligned}$$

对于每一固定的 v, 将里面的和分为 $\ll \dfrac{N}{Uq}+1$ 个长度都 $\leqslant q$ 的分和. 由于每一分和都 $\ll U+q\log q$ 及 $\log q<\log N=L$, 所以

$$\begin{aligned}
S^2\ll&UL^3(NU^{-1})(NU^{-1}q^{-1}+1)(U+q\log q)\\
\ll&N^2L^4(q^{-1}+qN^{-1}+U^{-1}+UN^{-1}).
\end{aligned}$$

我们概述下面的定理来作为Виноградов 方法的典型例子.

定理 1　命 $N\geqslant 1$, $L=\log N$ 及 $H=\mathrm{e}^{\frac{1}{2}\sqrt{L}}$, 又命

$$\left|a-\frac{h}{q}\right|<\frac{1}{q^2},\quad (h,q)=1,\ 1<q<N,$$

则

$$S(\alpha)=\sum_{p\leqslant N}\mathrm{e}^{2\pi\mathrm{i}ap}\ll NL^5\left(\sqrt{\frac{1}{q}+\frac{q}{N}}+\frac{1}{H}\right).$$

定理的证明可以划分为下面三个步骤.

1) (筛法). 命 $P=\prod\limits_{p\leqslant\sqrt{N}}p$ 为全体 $\leqslant\sqrt{N}$ 的素数的乘积, 则

$$\begin{aligned}S(a)&=\sum_{n\leqslant N}\Big(\sum_{d\mid(P,n)}\mu(d)\Big)\mathrm{e}^{2\pi\mathrm{i}an}+O(\sqrt{N})\\&=\sum_{d\mid P}\mu(d)\sum_{o\leqslant m\leqslant\frac{U}{d}}\mathrm{e}^{2\pi\mathrm{i}adm}+O(\sqrt{N}).\end{aligned}\tag{57}$$

将区间 $0<m\leqslant N$ 分为形如

$$M\leqslant m\leqslant M'$$

的子区间, 此处 $M<M'\leqslant 2M$, 这种区间的个数为 $O(L)$. 于是定理归结为去证明

$$S(M)=\sum_{d\mid P}\mu(d)\sum_{\substack{M<m\leqslant M'\\ m\leqslant\frac{N}{d}}}\mathrm{e}^{2\pi\mathrm{i}adm}\ll NL^4\Big(\sqrt{\frac{1}{q}+\frac{q}{N}}+\frac{1}{H}\Big).$$

2) (消去比较容易的部分). 当 $M\geqslant H$ 时,

$$S(M)\ll NL\Big(\frac{q}{N}+\frac{1}{q}+\frac{1}{H}\Big).$$

当 $M<H$ 时, $S(M)$ 中的与只含有 $\leqslant H^2$ 的素因子的 d 相应的各项之和显然 $\ll NH^{-1}$.

现在我们来研究和

$$\sum_{M<m\leqslant M'}\sum_{d\leqslant\frac{N}{m}}\mu(d)\mathrm{e}^{2\pi\mathrm{i}adm},$$

此处 $M<H$, 而 d 经过 P 的全体那种因子, 即至少含有一个 $>H^2$ 的素因子者. 将上面的和记为

$$\sum_k S_k'(M)-\sum_k S_k''(M),$$

此处

$$S_k'(M)=\sum_{M<m\leqslant M'}\sum_{d\leqslant\frac{N}{m}}\mathrm{e}^{2\pi\mathrm{i}adm},$$

而 d 经过 P 的满足下面条件的全体因子: $\mu(d)=1$, 而且 d 正好有 k 个素因子 $>H^2$. $S_k''(M)$ 的定义是类似的, 仅需在 $S_k'(M)$ 的定义中将 $\mu(d)=1$ 换为 $\mu(d)=-1$.

因为 $\leqslant N$ 的数最多只有 $\ll L$ 个素因子, 所以 k 的最大值亦 $\ll L$. 因此, 问题归结为去证明

$$S_k'(M)\ll NL^3\Big(\sqrt{\frac{1}{q}+\frac{q}{N}}+\frac{1}{H}\Big);$$

又对 $S_k''(M)$ 也有同样的估计.

3) 命

$$T_k(M) = \sum_{M<m\leqslant M'} \sum_{pt\leqslant \frac{M}{m}} \mathrm{e}^{2\pi\mathrm{i}aptm},$$

此处 p 通过适合 $H^2 < p \leqslant \sqrt{N}$ 的全体素数, 而 t 通过 P 的具有下面条件的全体因子; t 正好有 $k-1$ 个 $> H^2$ 的素因子而且 $\mu(t) = -1$. 于是

$$|S_k'(M)| \leqslant \frac{1}{k}|T_k(M)| + O(NH^{-2}) \leqslant |T_k(M)| + O(NH^{-2}).$$

为了估计 T_k, 我们将区间 $H^2 < p \leqslant \sqrt{N}$ 分成 $\ll L$ 个形为 $Q < p \leqslant Q'$ 的子区间, 此处 $Q < Q' \ll Q$. 因此, 只要证明

$$T_k(M,Q) = \sum_{M<m\leqslant M'} \sum_{Q<p\leqslant Q'} \sum_{mpt\leqslant N} \mathrm{e}^{2\pi\mathrm{i}aptm} \ll NL^2\Big(\sqrt{\frac{1}{q}+\frac{q}{N}}+\frac{1}{H}\Big)$$

便已足够.

现在来应用引理. 取 $u = mp,\ v = t$, 其中 t 满足上面所说的条件. 因为引理之 U 在此为 MQ, 故得

$$\begin{aligned} T_k(M,\ Q) \ll& NL^2(q^{-1}+qN^{-1}+M^{-1}Q^{-1}+MQN^{-1})^{\frac{1}{2}} \\ \ll& NL^2((q^{-1}+qN^{-1})^{\frac{1}{2}}+H^{-1}). \end{aligned}$$

定理证完.

Виноградов[116] 将他自己的定理推广为更一般的结果. 例如, 我们得到下面的定理.

定理 2 命 $0 < Q \leqslant C_1(k)L^{\sigma_2}$,

$$f(x) = \frac{h}{q}x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k, \quad (h,q) = 1,$$

此处 $\alpha_i (1 \leqslant i \leqslant k)$ 都是实数, 而 $L^\sigma < q \leqslant P^k L^{-\sigma}$. 则对任何 $\sigma_0 > 0$, 当 $\sigma > 2^{6k}\cdot(\sigma_0+\sigma_1+1)$ 时,

$$\left|\sum_{\substack{p\leqslant P\\ p\equiv t(\bmod\ Q)}} \mathrm{e}^{2\pi\mathrm{i}f(p)}\right| \leqslant C_2(k)PL^{-\sigma_0}Q^{-1}.$$

Turán[117] 证明了下面的估计等价于拟似 Riemann 猜想：当 $3 < |t|^\alpha \leqslant \frac{N}{2} \leqslant N_1 < N_2 \leqslant N,\ a \geqslant 4,\ 0 < \delta \leqslant \frac{1}{2}$ 时,

$$\max_{\frac{t}{10N}\leqslant y\leqslant \frac{3t}{N}} \left|\sum_{N_1\leqslant p\leqslant N_2} \mathrm{e}^{\mathrm{i}py}\right| \ll \frac{N\log^{10}N}{|t|^{\frac{1}{2}+\delta}}.$$

Виноградов[118] 也得到了关于素数变数的特征和的估计, 他在 1952 年得到了下面的结果:

定理 3 命 q 表一素数, $\chi(n)$ 为 mod q 的非主特征. 若 $q^{\frac{3}{4}} \ll N \ll q^{\frac{5}{4}}$, 则对适合 $k \not\equiv 0 \pmod q$ 的任何 k, 都有

$$\sum_{p \leqslant N} \chi(p+k) \ll N^{1+\varepsilon}\left(\frac{q^{\frac{3}{4}}}{N}\right)^{\frac{1}{4}},$$

此处 p 经过 $\leqslant N$ 的全体素数.

由定理 3 立刻得到

定理 4 命 n 为 $q-1$ 的一个因子, 且 $1<n<q-1$, s 为 0, 1, 2, $\cdots$, $n-1$ 中的一个; T_s 为适合下面条件的 $p+k$ 的个数:

$$p \leqslant N, \quad \operatorname{ind}(p+k) \equiv s \pmod n,$$

则在定理 3 的条件下有

$$T_s - \frac{1}{n}\pi(N) \ll N^{1+\varepsilon}\left(\frac{q^{\frac{3}{4}}}{N}\right)^{\frac{1}{4}}.$$

第3章　素数分布及与之相关的 Riemann ζ- 函数的性质

3.1　素 数 定 理

命 $\pi(x)$ 表示不超过 x 的素数个数. 从 $\pi(x)$ 的最初几个函数值看来, $\pi(x)$ 似乎很不规则, 但是随着数据的增加, 可以看到, 对于函数 $\pi(x)$, 可能有一渐近表示式. Legendre[119)] 猜想, 对于充分大的 $x, \pi(x)$ 渐近等于

$$\frac{x}{\log x - 1.08366}, \tag{58}$$

此处 $\log x$ 表示 x 的自然对数. Gauss[120)] 又独立地建议了一个类似而并不与它相等的公式. 以一千个连续整数为单位, Gauss 的方法在于计算每个单位中的素数个数, 他建议用函数 $\dfrac{1}{\log x}$ 来表示在大整数 x 附近的素数分布的平均密度 ("单位区间中素数的百分率"). 因此他用

$$\int_2^x \frac{\mathrm{d}u}{\log u} \tag{59}$$

来渐近表示 $\pi(x)$. 为了方便起见, 常常用"对数积分"

$$\mathrm{li}x = \lim_{\eta\to 0}\left(\int_0^{1-\eta} + \int_{1+\eta}^x\right)\frac{\mathrm{d}u}{\log u}$$

来代替上面的函数，这两个函数之差为一常数 $\mathrm{li}\,2 = 1.04\cdots$. 如果我们仅仅考虑主阶, 则这两个猜想都可以陈述为

$$\lim_{x\to\infty}\frac{\pi(x)}{\dfrac{x}{\log x}} = 1. \tag{60}$$

这就是通常所称的"素数定理". 这是素数分布理论中的中心定理. 近百年来, 决定素数定理真伪的问题, 吸引了不少数学家的注意.

首先在这个方向上作出重要贡献的是Чебышев[121)]. 他在 1848 年与 1850 年证明了

$$a \leqslant \varliminf_{x\to\infty}\frac{\pi(x)}{\dfrac{x}{\log x}} \leqslant 1 \leqslant \varlimsup_{x\to\infty}\frac{\pi(x)}{\dfrac{x}{\log x}} \leqslant \frac{6}{5}a, \tag{61}$$

此处 $a = 0.92129$. 亦即他证明了：如果极限存在, 则极限必定为 1; 而且当 x 充分大时, 这个比例界于两个正常数之间. 尽管Чебышев所得到的数值上界被以后的数学家不断地加以改进, 但这些数学家所用的方法, 似乎是不可能导至问题的最终解决的.

Чебышев引进了两个函数：

$$\vartheta(x) = \sum_{p \leqslant x} \log\ p \tag{62}$$

及

$$\psi(x) = \sum_{p^m \leqslant x} \log\ p = \sum_{n \leqslant x} \Lambda(n) = \vartheta(x) + \vartheta(x^{\frac{1}{2}}) + \vartheta(x^{\frac{1}{3}}) + \cdots, \tag{63}$$

此处

$$\Lambda(n) = \begin{cases} \log p, & \text{若}n\text{为素数}p\text{的方幂;} \\ 0, & \text{其他情形.} \end{cases}$$

他证明了下面两个公式都等价于素数定理：

$$\vartheta(x) \sim x \tag{64}$$

与

$$\psi(x) \sim x. \tag{65}$$

最后，我们引征 Sylvester[122) 的话来说明Чебышев贡献的意义以及他对这个问题的展望：

“但是要确立这种可能性的存在, 我们或许要等待在世界上产生这样一个人, 他的智慧与洞察力象Чебышев一样, 证明自己是超人一等的”.

当 Sylvester 写下这些东西的时候, Hadamard 出生了. 但是我们不应该仅仅归功于个别人的才华. 前人的劳动, 特别是 Riemann 的工作, 为他证明素数定理开辟了道路.

3.2　Riemann 的解析方法

Riemann[123) 在 1859 年提出的新思想是解决这个问题的钥匙, 他的名著的意义不仅在于素数论, 而且亦影响着一般函数论的发展, 他引入了处理复变函数 Riemann ζ- 函数

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s = \sigma + \mathrm{i}t, \tag{66}$$

的想法. Euler 在 1737 年将 $\zeta(s)$ 作为实变函数来研究. 他亦得到在素数分布论上的若干应用. 虽然 Riemann 的考虑主要并不在于 $\pi(x)$ 的渐近表示, 但他的分析已经明确指出了, 在这个函数与 $\zeta(s)$ 的性质间有着密切的联系, 特别与它在 s 平面上的零点分布有关. 但是在大多数情况下, Riemann 仅仅只给出了证明的不充分的指示. 为了说明他的名著的价值, 我们在这里概述一下他已经证明了的与猜想的结果.

由恒等式

$$\int_0^{\infty} x^{\frac{1}{2}s-1}\mathrm{e}^{-n^2\pi x}\mathrm{d}x=\frac{\Gamma\left(\frac{1}{2}s\right)}{\pi^{\frac{1}{2}s}}\cdot\frac{1}{n^s},\quad \sigma>0$$

出发, 我们得到: 当 $\sigma>0$ 时,

$$\frac{\Gamma\left(\frac{1}{2}s\right)\zeta(s)}{\pi^{\frac{1}{2}s}}=\sum_{n=1}^{\infty}\int_0^{\infty}x^{\frac{1}{2}s-1}\mathrm{e}^{-n^2\pi x}\mathrm{d}x=\int_0^{\infty}x^{\frac{1}{2}s-1}\psi(x)\mathrm{d}x$$

成立, 此处

$$\psi(x)=\sum_{n=1}^{\infty}\mathrm{e}^{-n^2\pi x}.$$

由于当 $x>0$ 时, $2\psi(x)+1=\frac{1}{\sqrt{x}}\left\{2\psi\left(\frac{1}{x}\right)+1\right\}$, 因此

$$\begin{aligned}\pi^{-\frac{1}{2}s}\Gamma\left(\frac{1}{2}s\right)\zeta(s)&=\int_0^1 x^{\frac{1}{2}s-1}\psi(x)\mathrm{d}x+\int_1^{\infty}x^{\frac{1}{2}s-1}\psi(x)\mathrm{d}x\\&=\frac{1}{s(s-1)}+\int_1^{\infty}\left(x^{-\frac{s}{2}-\frac{1}{2}}+x^{\frac{s}{2}-1}\right)\psi(x)\mathrm{d}x.\end{aligned}\tag{67}$$

最后的积分对于全体 s 都收敛, 故由解析延拓可知. 这个公式对于全体 s 都成立. 由于当 s 换为 $1-s$ 时, 公式 (67) 的右端不改变, 故得函数方程

$$\zeta(1-s)=\frac{2}{(2\pi)^s}\cos\frac{1}{2}\pi s\Gamma(s)\zeta(s).\tag{68}$$

由 (67) 可见, $\zeta(s)$ 除了在 $s=1$ 处有一个残数为 1 的一次极外, 它在整个平面上是正则的. 又因当 $\sigma>1$ 时,

$$\zeta(s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1},\tag{69}$$

此处 p 经过全体素数, 故当 $\sigma>1$ 时, $\zeta(s)$ 没有零点. 因此由 (68) 可知, 当 $\sigma<0$ 时, $\zeta(s)$ 除了在 $s=-2,-4\cdots$ 处有一次零点之外, 它没有其他零点. 我们称这些

零点为 $\zeta(s)$ 的"无聊零点". $\zeta(s)$ 可能有的其他零点 $\rho_1, \rho_2 \cdots$ 都位于带状区域 $0 \leqslant \sigma \leqslant 1$ 之中. 因为

$$(1-2^{1-s})\zeta(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots > 0, \quad 0 < s < 1 \tag{70}$$

及 $\zeta(0) \neq 0$, 所以 $\zeta(s)$ 在 0 与 1 之间的实轴段上没有零点, 亦即 ρ_1, ρ_2, $\cdots$ 都是复数.

这些就是 Riemann 名著上已经证明了的关于函数 $\zeta(s)$ 的性质. 他还提出了如下的猜想:

1) $\zeta(s)$ 在带状区域 $0 \leqslant \sigma \leqslant 1$ 中有无穷多个零点;

2) 若 $N(T)$ 表示 $\zeta(s)$ 在矩形 $0 \leqslant \sigma \leqslant 1, 0 < t < T$ 中的零点个数, 则

$$N(T) = \frac{1}{2\pi} T \log T - \frac{1 + \log(2\pi)}{2\pi} T + O(\log T);$$

3) 若以 $\rho = \beta + \mathrm{i}\gamma$ 来一般标记 $\zeta(s)$ 的非无聊零点, 则 $\sum |\rho|^{-2}$ 收剑, 而 $\sum |\rho|^{-1}$ 发散;

4) 整函数

$$\xi(s) = \pi^{-\frac{1}{2}s}(s-1)\zeta(s)\Gamma\left(\frac{s}{2}+1\right)$$

可以表为

$$a\mathrm{e}^{bs} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) \mathrm{e}^{\frac{s}{\rho}},$$

此处 $\prod_{\rho}$ 为绝对收敛的无穷乘积, 其中 ρ 经过 $\zeta(s)$ 的全体非无聊零点;

5) $\zeta(s)$ 的全体非无聊零点都位于直线 $\sigma = \dfrac{1}{2}$ 上;

6) 命 $\Pi(x) = \sum\limits_{2 \leqslant n \leqslant x} \dfrac{\Lambda(n)}{\log n}$ 及 $\Pi_0(x) = \dfrac{1}{2}(\Pi(x+0) + \Pi(x-0))$. 则有公式

$$\Pi_0(x) = \mathrm{li}\ x - \sum_{\rho} \mathrm{li}\ x^{\rho} + \int_x^{\infty} \frac{\mathrm{d}u}{(u^2-1)u\log u} - \log 2, \quad x > 1,$$

此处 $\mathrm{li}\ x^{\rho} = \mathrm{li}\ \mathrm{e}^{\rho \log x}$ 及

$$\mathrm{li}\ \mathrm{e}^{w} = \int_{-\infty+v\mathrm{i}}^{u+v\mathrm{i}} \frac{\mathrm{e}^z \mathrm{d}z}{z}, \quad w = u + \mathrm{i}v, \quad v \gtrless 0.$$

这就是 Riemann 的素数公式.

3.3　Hadamard 与 von Mangoldt 的贡献

Hadamard[124] 在 1892 年与 1893 年发表了两篇极为重要的整函数论的论文. 他证明了: $\xi(s)$ 是阶等于 1 的整函数, 或者更进一步, 由 §17, (67) 可以导出 $\xi(s) = O(\mathrm{e}^{A|s|\log|s|})$. 因此, Hadamard 在第二篇论文之末解决了 Riemann 的猜想 1), 3), 4). 在 4) 中, 我们有 $a = \frac{1}{2}, b = \log 2 + \frac{1}{2}\log \pi - 1 - \frac{1}{2}\gamma$, 此时 γ 为 Euler 常数. Hadamard[125] 与de la Vallée Poussin[126] 在 1896 年, 几乎同时而又相互独立地证明了素数定理.

von Mangoldt[127] 证明了Riemann的另外两个猜想 2) 与 6). 由"辐角原理"可知, $\zeta(s)$($\xi(s)$ 亦然) 在以 $2\pm\mathrm{i}T$ 及 $-1\pm\mathrm{i}T$ 为顶点的矩形中的零点个数 $2N(T)$ 等于

$$\frac{1}{2\pi}[\arg \xi(s)]_c,$$

此处 $[\arg \xi(s)]_c$ 表示当 s 以正向沿矩形的周界 C 走一周时，辐角 $\arg \xi(s)$ 的增加量. 显然

$$[\arg \xi(s)]_c = \left[\arg\frac{1}{2}\ s(s-1)\right]_c + [\arg\Phi(s)]_c,$$

此处 $\Phi(s) = \pi^{-\frac{1}{2}s}\Gamma\left(\frac{1}{2}s\right)\zeta(s)$. 右端的第一项等于 4π. 又因为 $\Phi(s)$ 在点 s 与点 $1-s$ 处取等值, 在点 $\sigma+\mathrm{i}t$ 及 $\sigma-\mathrm{i}t$ 处取共轭值, 故第二项显然等于 $4[\arg\Phi(s)]_{\mathcal{L}}$, 此处 $\mathcal{L}$ 为由 2 至 $2+\mathrm{i}T$ 的线段 $\mathcal{L}_1$ 及由 $2+\mathrm{i}T$ 至 $\frac{1}{2}+\mathrm{i}T$ 的线段 $\mathcal{L}_2$ 所构成的折线. 因此

$$\pi N(T) = \pi + [\arg \pi^{-\frac{1}{2}s}]_{\mathcal{L}} + \left[\arg \Gamma\left(\frac{1}{2}s\right)\right]_{\mathcal{L}} + [\arg \zeta(s)]_{\mathcal{L}}. \tag{71}$$

首先, 我们有

$$[\arg \pi^{-\frac{1}{2}s}]_{\mathcal{L}} = \left[-\frac{1}{2}t \log \pi\right]_{\mathcal{L}} = -\frac{1}{2}T \log \pi.$$

其次, 由复数形式的 Stirling 公式可知, 当 $T\to\infty$ 时,

$$\begin{aligned}\left[\arg \Gamma\left(\frac{1}{2}s\right)\right]_{\mathcal{L}} &= \Im \log \Gamma\left(\frac{1}{4}+\frac{1}{2}\mathrm{i}\ T\right) - \Im\ \mathrm{rog}\ \Gamma(1)\\ &= \frac{1}{2}\ T \log\frac{T}{2} - \frac{\pi}{8} - \frac{T}{2} + O(T^{-1}).\end{aligned}$$

代入 (71) 式便得

$$N(T) = \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + \frac{7}{8} + \frac{1}{\pi}[\arg\zeta(s)]_{\mathcal{L}} + O\left(\frac{1}{T}\right).$$

因此, 猜想 2) 的证明就归结为下式的证明:

$$\zeta(T) = \frac{1}{2}\ [\arg \zeta(s)]_{\mathcal{L}} = O(\log T).$$

这个公式是下面的关于解析函数的引理的推论. 而这引理本质上是属于Backlund[128)]的.

引理　命 $0 \leqslant \alpha < \beta < 2$; $f(s)$ 为一解析函数, 它当 s 为实数时取实值, 又当 $\sigma \geqslant \alpha$ 时, 除 $s = 1$ 外, 为正则的. 又命

$$|\Re f(2 + it)| \geqslant m > 0$$

及

$$|f(\sigma' + it')| \leqslant M_{\sigma,t}, \quad \sigma' \geqslant \sigma,\ 1 \leqslant t' \leqslant t.$$

若 T 并非 $f(s)$ 零点的纵坐标, 则当 $\sigma \geqslant \beta$ 时,

$$|\arg f(\sigma + iT)| \leqslant \pi\Big(\log M_{\alpha,T+2} + \log \frac{1}{m}\Big)/\log\{(2-\alpha)/(2-\beta)\} + \frac{3\pi}{2}.$$

Backlund的方法与von Mangoldt的证明不一样, 它不依赖于Hadamard 的供献. 从而也就给Riemann 的猜想 1) 与 3) 提供了另一证明. 实际上, 我们可以得到比 3) 更精密的关于零点分布的结果：当 $\alpha > 2$ 时, $\sum |\rho|^{-1}(\log|\rho|)^{-\alpha}$ 收敛, 而当 $\alpha \leqslant 2$ 时, 这级数发散. 并且有

$$\sum_{0<\gamma\leqslant T} \frac{1}{\gamma} = O(\log^2 T) \tag{72}$$

与

$$\sum_{\gamma>T} \frac{1}{\gamma^2} = O\Big(\frac{\log T}{T}\Big). \tag{73}$$

von Mangoldt 最重要的贡献是他证明了Riemann 的素数公式 (猜想 6)). von Mangoldt也证明了下面类似的公式.

定理 1　命 $\psi_0(x) = \frac{1}{2}(\psi(x+0) + \psi(x-0))$. 则当 $x > 1$ 时,

$$\psi_0(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{1}{2}\log\Big(1 - \frac{1}{x^2}\Big), \tag{74}$$

此处和号 $\sum\limits_\rho$ 表示当 $T \to \infty$ 时,

$$S(x,T) = \sum_{|\gamma|\leqslant T} \frac{x^\rho}{\rho}$$

的极限.

如果将上面的级数逐项积分, 便得

定理 2　当 $x>1$ 时,

$$\psi_1(x)=\int_0^x \psi(t)\mathrm{d}t=\frac{1}{2}x^2-\sum_{\rho}\frac{x^{\rho+1}}{\rho(\rho+1)}-x\,\frac{\zeta'}{\zeta}(-1)-\sum_{r=1}^{\infty}\frac{x^{1-2r}}{2r(2r-1)},\tag{75}$$

此处级数 $\sum\limits_{\rho}$ 是绝对收敛的.

定理 2 的证明较定理 1 的证明容易, 在这里, 我们仅仅概述一下 (75) 式的证明.

先叙述一下 $\zeta(s)$ 的两个性质.

1) 存在数贯 $T_2, T_3, \cdots$ 满足

$$m<T_m<m+1,\quad m=2,3,\cdots$$

及

$$\frac{\zeta'}{\zeta}(s)\ll \log^2 t,\quad -1\leqslant\sigma\leqslant 2,\quad t=T_m.$$

2) 在区域 $\sigma\leqslant -1, |s-n|\geqslant \frac{1}{2}$, $n=-2,-4,-6,\cdots$ 中, 有

$$\frac{\zeta'}{\zeta}(s)\ll \log(|s|+1).$$

习知

$$\psi_1(x)=-\lim_{m\to\infty}\frac{1}{2\pi \mathrm{i}}\int_{2-T_m\mathrm{i}}^{2+T_m\mathrm{i}}\frac{x^{s+1}}{s(s+1)}\frac{\zeta'}{\zeta}(s)\mathrm{d}s.$$

由性质 1) 与 2), 将积分直线 $2+t\mathrm{i}(|t|\leqslant T_m)$ 换为折线:

$$-2m-1\pm t\mathrm{i}(|t|\leqslant T_m),\quad \sigma\pm \mathrm{i}T_m(-(2m+1)\leqslant\sigma\leqslant 2),$$

在以 $2\pm T_m i$, $-2m-1\pm T_m i$ 为顶点的矩形中，各个残数之和为

$$\frac{1}{2}x^2-\sum_{|\gamma|<T_m}\frac{x^{\rho+1}}{\rho(\rho+1)}-x\frac{\zeta'}{\zeta}(0)+\frac{\zeta'}{\zeta}(-1)-\sum_{r=1}^{m}\frac{x^{-2r+1}}{(-2r)(-2r+1)}.$$

于是命 $m\to\infty$, 便得 (75) 式.

因此, 在Riemann的这些猜想中, 除猜想 5) 外, 都已获得解决. 猜想 5) 就是当今著称的Riemann猜想. 从现在开始, 所谓Riemann猜想就是指猜想 5).

3.4　有误差项的素数定理

素数分布理论的中心问题是寻求

$$\pi(x) - \text{li } x$$

或

$$\psi(x) - x$$

的最佳误差.

在Riemann猜想下, von Koch[129] 证明了

$$\psi(x) = x + O(x^{\frac{1}{2}} \log^2 x). \tag{76}$$

事实上, 由 §18, (75) 式得到

$$\begin{aligned}\pm(\psi_1(x \pm 1) - \psi_1(x)) =& x + O\left(\left|\sum_{\rho} \frac{(x \pm 1)^{\rho+1} - x^{\rho+1}}{\rho(\rho+1)}\right|\right) + O(1) \\ =& x + O\left(\sum_{|\rho| \leqslant x} \frac{1}{|\rho|}\left|\int_x^{x\pm1} u^{\rho} du\right|\right) + O\left(\sum_{|\rho|>x} \frac{(x+1)^{\frac{3}{2}}}{|\rho(\rho+1)|}\right) \\ =& x + O\left(x^{\frac{1}{2}} \sum_{|\gamma| \leqslant x} \frac{1}{|\gamma|}\right) + O\left(x^{\frac{3}{2}} \sum_{|\gamma|>x} \frac{1}{|\gamma|^2}\right) \\ =& x + O(x^{\frac{1}{2}} \log^2 x)\end{aligned}$$

(其中用到 §18, (72), (73) 式). 因为

$$\psi_1(x) - \psi_1(x-1) = \int_{x-1}^{x} \psi(t)\mathrm{d}t \leqslant \psi(x) \leqslant \int_x^{x+1} \psi(t)\mathrm{d}t = \psi_1(x+1) - \psi_1(x),$$

故得 (76) 式. 从而也得到

$$\pi(x) = \text{li } x + O(x^{1/2} \log x). \tag{77}$$

定理 1　若 $\zeta(s)$ 在区域

$$\sigma > 1 - \eta(|t|)$$

中无零点, 此处当 $t \geqslant 0$ 时, $\eta(t)$ 为正的递减函数, 则

$$\psi_1(x) = \frac{1}{2} x^2 + O(x^2 \mathrm{e}^{-aw(x)}),$$

此处 a 为适合 $0 < a < 1$ 的固定常数, $\omega(x) = \eta(t)\log x$, 而当 $t > 0$ 时, t 由等式 $\eta(t)\log x = \log t$ 来定义.

事实上, 因为 $x^{-\eta(\gamma)}$ 的递减性及 $x^{-\eta(\gamma)} \leqslant 1$, 故由 §18, (75) 得

$$\psi_1(x) - \frac{1}{2}x^2 \ll x^2\left(\sum_{|\gamma|\leqslant T}\frac{1}{|\gamma|^2}x^{-\eta(T)} + \sum_{|\gamma|>T}\frac{x^{-\eta(\gamma)}}{|\gamma|^2}\right)$$
$$\ll x^2\left(x^{-\eta(T)} + \frac{\log T}{T}\right) \ll x^2\mathrm{e}^{-aw(x)}. \tag{78}$$

由 (78) 得

$$\psi(x) = x + O(x\mathrm{e}^{-\frac{1}{2}aw(x)}), \tag{79}$$

与

$$\pi(x) = \mathrm{li}\ x + O(x\mathrm{e}^{-\frac{1}{2}aw(x)}). \tag{80}$$

Turán[117] 在 $\zeta(s)$ 的无零点区域与 $\pi(s) - \mathrm{li}\ x$ 的阶之间建立了一个紧密关系.

de la Vallée Poussin[130] 证明了：对于

$$\eta(t) = \frac{a}{\log(t+1)}, \quad t \geqslant 1,$$

定理 1 的假定成立, 故得

$$\pi(x) = \mathrm{li}\ x + O(x\mathrm{e}^{-a\sqrt{\log x}}). \tag{81}$$

Littlewood[131] 首先引进了估计指数和的方法来改进 $\zeta(s)$ 的无零点区域, 从而他证明了可以用较佳的误差

$$O(x\mathrm{e}^{-a\sqrt{\log\ x\log\ \log x}})$$

来代替 (81) 式的误差.

应用Виноградов 关于三角和估计的结果, Чудаков[132], Titchmarsh[133] 及Виноградов[24] 等人得到了更进一步的结果. 最佳的结果为：

定理 1 的假定对于

$$\eta(t) = \frac{A}{(\log\ t)^{\frac{2}{3}+\varepsilon}}$$

成立，从而得到

$$\pi(x) = \mathrm{li}\ x + O(x\mathrm{e}^{-\alpha(\log\ x)^{\frac{3}{5}+\varepsilon}})^{24)},$$

此处 ε 与 α 为任意给定的正数, 而与记号 O 有关的常数仅依赖于 α 及 ε. Landau 提供了另一个比较初等的、不依赖于von Mangoldt公式的处理上述结果的方法. Rosser[134] 还得到一些数值定理, 即

$$\frac{x}{\log\ x} < \pi(x) < \frac{x}{\log\ x - 2}, \quad 若17 \leqslant x \leqslant \mathrm{e}^{100}, \quad x \geqslant \mathrm{e}^{2000};$$

$$\frac{x}{\log x+2}<\pi(x)<\frac{x}{\log x-4},\quad 若 x>55;$$
$$p_n>n\log n,\qquad 若 n\geqslant 1,$$

此处 p_n 表示第 n 个素数.

3.5　素数定理误差项的不规则性

由数值计算可以看出, 似乎应该有

$$\pi(x)<\mathrm{li}\ x$$

(见Ingham[135] 的书), 例如证明了 $\pi(10^9)<\mathrm{li}\ 10^9$. 但是Littlewood[136] 在 1914 年证明了有充分大的 x, 满足 $\pi(x)>\mathrm{li}\ x$, 而这样的 x 将要出现无穷多次. Littlewood 的定理纯粹是一个“存在定理”. 以后, Skewes[137] 在Riemann 猜想下证明了: 存在适合 $x<\mathrm{e}^{\mathrm{e}^{\mathrm{e}^{7.703}}}$ 的整数 x, 使

$$\pi(x)>\mathrm{li}\ x.$$

在不假定Riemann 猜想时, 他证明了有整数 $x<10^{10^{10^{10^3}}}$ 也具有此同一性质.

如果存在与 x 无关的正常数 c, 使有任意大的 x 满足 $|f(x)|>cx$, 则用记号

$$“f(x)=\Omega(x),\quad 当 x\to\infty”$$

表之. 因此“Ω”是“O”的逆记号. 若 $f(x)$ 为实函数, 且有任意大的 x 使 $f(x)>cx$, 则记为

$$f(x)=\Omega_+(x),$$

又若有任意大的 x, 使 $f(x)<-cx$, 则记为

$$f(x)=\Omega_-(x).$$

因此“Ω”等价于 (对于实函数)“或者 Ω_+, 或者 Ω_-”. 用记号“$\Omega_\pm$”表示“$\Omega+$ 与 Ω_- 的全体”.

Schmidt[138] 证明了, 如果在 $\sigma>\Theta>\frac{1}{2}$ 中, $\zeta(s)$ 没有零点, 则对于任意的 $\delta>0$, 有

$$\psi(x)-x=\Omega_\pm(x^{\Theta-\delta})$$

及

$$\pi(x)-\mathrm{li}\ x=\Omega_\pm(x^{\Theta-\delta}).$$

Pólya[139] 得到更精确的结果：命 $w(n)$ 表示在贯 $\psi(1)-1,\psi(2)-2,\cdots,\psi(n)-n$ 中出现的变号次数, 则

$$\overline{\lim_{n\to\infty}}\frac{w(n)}{\log n}>\frac{c}{\pi},$$

此处 c 的定义如下：若 $\zeta(s)$ 在直线 $\sigma=\Theta$ 上有零点, 则 c 为这些零点的最小正虚部 γ, 否则 $c=\infty$.

Littlewood[140] 证明了：当 $x\to\infty$ 时, 有

$$\psi(x)-x=\Omega_{\pm}(x^{\frac{1}{2}}\log\log\log x)$$

与

$$\pi(x)-\mathrm{li}\ x=\Omega_{\pm}\left(\frac{x^{\frac{1}{2}}}{\log x}\log\log\log x\right).$$

3.6 相继二素数之差距

设 p_n 是第 n 个素数. 今往研究相继二素数之差距

$$d_n=p_{n+1}-p_n$$

的分布问题. 有两个主要问题：

1) 设法找一函数 $f_1(n)$, 使对全体大 n,

$$d_n\ll f_1(n)$$

成立. 在这方面, 已知的最优结果本质上属于Ingham[141], 此即 $f_1(n)=p_n^{\Theta},\Theta=\dfrac{38}{61}+\varepsilon$.

在Riemann猜测成立的假定下, Cramér[142] 证明了 $f_1(n)=p_n^{\frac{1}{2}}\log p_n$. 它的反面问题是去寻找函数 $f_2(n)$, 使对无限多个 n,

$$d_n\geqslant f_2(n)$$

成立. 对于这个问题, Rankin[143] 得到了迄今为止的最优结果：

$$f_2(n)=\left(\frac{1}{3}-\varepsilon\right)\log p_n\log\log p_n\frac{\log\log\log\log p_n}{(\log\log\log p_n)^2},$$

他所用的是初等方法.

Western[144] 公布了一张表, 表中包含了这种素数 $p_n: p_n\leqslant 10^7$, 而它们的 d_n 大于一切更小素数之差距. 这种素数一共只有 20 个, 其中最大的是 4652353, 在它那里的差距等于 154. 这张表支持了下面的猜测, 即

$$f_1(n)=p_n^{\frac{1}{2}+\varrho}\quad 及\ f_2(n)=3(\log_{10}p_n)^2.$$

2) 设法找一函数 $f_3(n)$, 使对全体大 n,

$$d_n \geqslant f_3(n)$$

成立. 关于 $f_3(n)$, 我们还一无所知; 但若有关孪生素数的猜测真确, 就有 $f_3(n) = 2$. 相反地, 我们要找一函数 $f_4(n)$, 使对无限多个 n,

$$d_n \leqslant f_4(n)$$

成立. Rankin[145)] 用Бухштаб[46)] 的方法建立了下面的结果：对于任何 $\varepsilon > 0$, 都有 $f_4(n) = \left(\frac{57}{59} + \varepsilon\right)\log p_n$; 而在广义Riemann猜测的假定下, 他还证明了 $f_4(n) = \left(\frac{42}{43} \times \frac{3}{5} + \varepsilon\right)\log p_n$. Ricci[146)] 证明：对于固定的 $\delta(0 < \delta < 1)$, 及时充分大的 N, 在区间 $(1-\delta)N < p_n \leqslant N$ 中, 至少有千分之五十五的差距 $p_{n+1} - p_n$ 适合不等式

$$p_{n+1} - p_n < \log p_n.$$

另一类问题是去寻找 $f_5(n)$, 使对几乎全体 n,

$$d_n \geqslant f_5(n)$$

成立. 所谓“对几乎全体 n 成立”, 它的意思是说, 适合上述不等式的 $n \leqslant x$ 的个数 $\sim x$.

Walfisz[147)] 证明了

$$f_5(n) = \log p_n\ (\log\log\log p_n)^{-2},$$

而Prachar[148)] 给出了稍更精确的结果：

$$f_5(n) = \frac{\log p_n}{g(p_n)},$$

此处 $g(x)$ 为一在 $x > x_0$ (x_0 为一正数) 时单调且当 $x \to \infty$ 时适合 $g(x) \to \infty$ 与 $\frac{\log x}{g(x)} \to \infty$ 的函数.

此外, 我们还要寻找函数 $f_6(n)$, 使

$$d_n \leqslant f_6(n)$$

对几乎全体 n 都成立. 关于这个问题, Cramér[149)] 建立了下面的结果：

对于

$$0 \leqslant \alpha < \frac{1}{2}, \quad \beta \geqslant 0, \quad h = x^{\alpha}(\log x)^{\beta},$$

在黎曼猜测真确的假定下, 可有

$$\frac{1}{x}\sum_{\substack{d_n>h\\ p_n\leqslant x}} d_n = O\left(\frac{\log^3 x}{h\log h}\right).$$

由此得到

$$f_6(n)\leqslant(\log n)^3.$$

在此同一假定下, Selberg[150] 证明了: 对于 $0\leqslant\alpha<1,\ \beta>0$, 可有

$$\frac{1}{x}\sum_{\substack{d_n>\frac{h}{x}p_n\\ p_n\leqslant x}} d_n = O\Big(\frac{\log^2 x}{h}\Big).$$

由于它的重要性, 我们将对 $f_1(n)$ 给出下面的证明过程, Hoheisel[151] 首先证明: 有绝对常数 $\Theta<1$ 存在, 使当 $x\to\infty$ 时,

$$\pi(x+x^{\Theta})-\pi(x)\sim\frac{x^{\Theta}}{\log x} \tag{82}$$

成立. 由此得出: 当 $n\to\infty$ 时,

$$d_n=O(p_n^{\Theta}). \tag{83}$$

他的证明能够叙述成下面的一般形式:

我们假定: $(a)\zeta(s)$ 在区域

$$\sigma>1-A\frac{\log\ \log t}{\log t},\quad A>0,\ t>t_0>\xi$$

中没有零点; (b) 当 $T\to\infty$ 时,

$$N(\sigma,T)=O(T^{b(1-\sigma)}\log^B T),\quad b>0,\ B\geqslant 0$$

关于 $\frac{1}{2}\leqslant\sigma\leqslant 1$ 一致地成立, 此处 $N(\sigma,T)$ 表示 $\zeta(s)$ 的零点 $\rho=\beta+i\gamma$ 之适合 $\beta\geqslant\sigma,0\leqslant\gamma\leqslant T$ 者之个数. 于是, 对于满足不等式

$$1-\frac{1}{b+A^{-1}B}<\Theta<1$$

的任何固定的 Θ, (82) 与 (83) 都成立.

我们从等式

$$\psi(x)=x-\sum_{|\gamma|<T}\frac{x^{\rho}}{\rho}+O\Big(\frac{x}{T}\log^2 x\Big)$$

出发, 此式在 $x \to \infty$ 时关于 $3 \leqslant T \leqslant x$ 一致地成立, 式中 $\psi(x)=\sum\limits_{p^m \leqslant x} \log p$, 而 $\rho=\beta+i\gamma$ 表示 $\zeta(s)$ 的复零点. 由此可以得到

$$\psi(x+h)-\psi(x)=h-\sum_{|\gamma|<T} \frac{(x+h)^{\rho}-x^{\rho}}{\rho}+O\Big(\frac{x}{T}\log^2 x\Big),$$

当 $x \to \infty$ 时, 记号 O 关于 $3 \leqslant T \leqslant x, 0<h \leqslant x$ 为一致的. 因为

$$\left|\frac{(x+h)^{\rho}-x^{\rho}}{\rho}\right|=\left|\int_x^{x+h} u^{\rho-1} \mathrm{d} u\right| \leqslant \int_x^{x+h} u^{\beta-1} \mathrm{d} u \leqslant h x^{\beta-1},$$

故得

$$\frac{\psi(x+h)-\psi(x)}{h}=1+O\Big(\sum_{|\gamma|<T} x^{\beta-1}\Big)+O\Big(\frac{x}{T\, h}\log^2 x\Big). \tag{84}$$

因为 $\zeta(s)$ 只有有限多个适合 $\frac{1}{2} \leqslant \beta<1,|\gamma| \leqslant t_0$ 的零点 $\rho=\beta+i\gamma$, 并且它没有零点适合 $\beta \geqslant 1$, 故由假定 (a), 一定能够找到 $T_0>0$, 使在 $T \geqslant T_0$ 与 $\sigma>1-\eta(T)$ 中, 有 $N(\sigma, T)=0$, 此处 $\eta(T)=A \log \log T / \log T$.

又因 $N\Big(\frac{1}{2}, T\Big) \gg T \log T$, 故若在假定 (b) 中取 $\sigma=\frac{1}{2}$, 可见 $b \geqslant 2$. 由 $N(0, T)=O(T \log T)$, 我们得到

$$\begin{aligned}
\sum_{|\gamma|<T} x^{\beta-1} & =2 x^{-1} N(0, T)+2 \int_0^1 N(\sigma, T) x^{\sigma-1} \log x \mathrm{d} \sigma \\
& \ll x^{-1} T \log T+\int_0^{1-\eta(T)}\Big(\frac{T^b}{x}\Big)^{1-\sigma} \log^B T \log x\, \mathrm{d} \sigma,
\end{aligned}$$

它在 $x \to \infty$ 时关于 $T_0 \leqslant T \leqslant x$ 一致地成立.

取 $T=x^{\alpha}, \alpha$ 为一适合 $0<\alpha<b^{-1}\Big(\leqslant \frac{1}{2}\Big)$ 的常数, 则得

$$\sum_{|\gamma|<T} x^{\beta-1}=O(x^{\alpha-1} \log x)+O(x^{(\alpha b-1) \eta(x^{\alpha})} \log^B x)=O((\log x)^{-\delta}),$$

此处 $\delta=(\alpha^{-1}-b) A-B$. 又取 α 使适合 $\alpha^{-1}>b+A^{-1} B(\geqslant b)$, 则有 $\delta>0$, 故若 $h=x^{\Theta}$ 而 $1>\Theta>1-\alpha\Big(>\frac{1}{2}\Big)$, 则当 $x \to \infty$ 时, 可有

$$\psi(x+h)-\psi(x) \sim h .$$

又因

$$\psi(x+h)-\psi(x)=\sum_{x<p \leqslant x+h} \log p+O\Big(\sum_{p^2 \leqslant x+h} \log p\Big[\frac{\log (x+h)}{\log p}\Big]\Big)$$

$$= \sum_{x<p\leqslant x+h} (\log x + O(1)) + O\bigg(\sum_{p^2\leqslant 2x} \log 2x\bigg)$$
$$=(\pi(x+h)-\pi(x))(\log x + O(1)) + O(x^{\frac{1}{2}}\log x),$$

故前式包含了 (82) 式, 因此也包含了 (83) 式.

Hoheisel[151] 利用了Littlewood[131] 的一个定理与Calson 的某一定理的改进. 前者隐含着有一数值 A 使 (a) 正确, 而后者保证 (b) 对 b=4, B=6 成立, 由此他证明了 $\Theta = \dfrac{32999}{33000}$. Heilbronn[152] 通过增加 A 的数值而将此结果改进到 $\dfrac{249}{250}$. 借助于Виноградов关于指数和的估计, Чудаков[153] 证明了 (a), 其中的 $A = A(t)$ 随 t 趋向无穷, 由此得到 $\Theta = \dfrac{3}{4} + \varepsilon$. 因此现在的任务在于改进 (b). 事实上, Ingham[141] 证明了 $N(\sigma,T) \ll T^{2(1-\sigma)(1+2c)}\log^5 T$ 此处 c 为使 $\zeta\Big(\dfrac{1}{2}+it\Big) = O(|t|^c)$ 成立的一个正数, 也即 (b) 对 $b = 2(1+2c)$ 与 $B = 5$ 正确. 因此我们得到 $\Theta = \dfrac{1+4c}{2+4c} + \varepsilon$. 关于 c 的已知最优结果是闵嗣鹤 [79] 得到的 $c = \dfrac{15}{92} + \varepsilon$, 由此 $\Theta = \dfrac{38}{61} + \varepsilon$.

注意, 为了眼下的应用, 关于 $N(\sigma,T)$ 的不等式只在 $\sigma = 1$ 的附近才令人感到兴趣. Turán[154] 对Calson 的公式作出了重要的贡献: 对于某一正的数值常数 b,

$$N(\sigma,T) \ll T^{2(1-\sigma)+6(1-\sigma)^{1.1}}$$

在 $1-b \leqslant \sigma \leqslant 1$ 及 $T > 3$ 中成立.

此外, 如果我们利用Lindelöf 猜测, 也即对于任何 $\varepsilon > 0$, 如果都有 $\zeta\Big(\dfrac{1}{2}+\mathrm{it}\Big) = O(|t|^\varepsilon)$, 则有 $\Theta = \dfrac{1}{2} + \varepsilon$. 在Riemann 猜测正确的假定下, 我们 [141),142] 能够证明

$$p_{n+1} - p_n = O(p_n^{\frac{1}{2}}\log p_n).$$

因若命

$$\Delta_h^{(2)} f(x) = f(x+2h) - 2f(x+h) + f(x),$$

则由 §18 的定理 2, 并用平凡的估计

$$\left|\frac{\Delta_h^{(2)} x^{\rho+1}}{\rho(\rho+1)}\right| \ll \min\bigg(h^2 x^{-\frac{1}{2}}; \frac{x^{\frac{3}{2}}}{\gamma^2}\bigg), \quad 1 \leqslant h \leqslant x,$$

可得

$$\Delta_h^{(2)} \psi_1(x) = h^2 + O(x \log^2 x).$$

取 $h = Cx^{\frac{1}{2}} \log x$, C 为充分大的绝对常数, 就得到上面的论断.

借助于一个以概率理论为基础的具有启发性的方法 [155], H. Cramér认为: 对于相继素数之差距, 可以猜想它们适合不等式

$$p_{n+1} - p_n \ll (\log p_n)^2.$$

3.7　素数在等差级数中的分布

以上各节的大多数结果, 都能推广到等差级数中的素数分布问题. 设 $q \geqslant 1$, l 为一适合 $0<l<q$ 与 $(q,l)=1$ 的整数. 用 $\pi(x;q,l)$ 表示不大于 x 并且 $\equiv l(\bmod q)$ 的素数个数, 也即

$$\pi(x;q,l)=\sum_{\substack{p\equiv l(\bmod q)\\ p\leqslant x}} 1.$$

又命

$$\vartheta(x;q,l)=\sum_{\substack{p\equiv l(\bmod q)\\ p\leqslant x}} \log p$$

及

$$\psi(x;q,l)=\sum_{\substack{n\equiv l(\bmod q)\\ n\leqslant x}} \Lambda(n).$$

对于 $\sigma>1$, 我们定义函数

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s},$$

它有很多性质与 $\zeta(s)$ 的相似.

Чудаков[156) 证明了

$$\psi(x;q,l)=\frac{x}{\varphi(q)}+E(q)\frac{\chi_1(l)}{\varphi(q)\sigma_1}-\frac{1}{\varphi(q)}\sum_{\chi}\bar{\chi}(l)\sum_{|\gamma|\leqslant T}\frac{x^{\rho}}{\rho}+O\left(\frac{x\log^2 x}{T}\right),$$

这里的 $E(q)$ 或等于 1, 或等于 0, 完全根据有没有使 $L(s,\chi_1)$ 在 $\sigma_1>1-\dfrac{c_1}{\log q}$ 中具有实零点的实特征 $\chi_1(n)\ (\bmod q)$ 而定. 又 $\rho=\beta+\mathrm{i}\gamma$ 表示 $L(s,\chi)$ 的零点, 而含在记号 O 中的常数则与 q 无关.

如果有模 q 特征的全体Dirichlet L- 函数在区域

$$\sigma>1-\frac{A}{\log(|t|+2)^{\frac{2}{3}}}$$

中都没有零点, 则用 §19 中的方法, 我们得到

$$\psi(x;q,l)=\frac{1}{\varphi(q)}x+O(x\mathrm{e}^{-c(\log x)^{\frac{3}{5}-\varepsilon}}),$$

记号 O 中所含的常数与 q 及 ε 有关. 我们也能证明

$$\pi(x;q,l)=\frac{1}{\varphi(q)}\mathrm{li}\ x+O(x\mathrm{e}^{-c(\log x)^{\frac{3}{5}-\varepsilon}})$$

及

$$p_{n+1}-p_n=O(p_n^{\frac{38}{61}+\varepsilon}),$$

此处 p_n 表等差级数 $\equiv l(\bmod q)$ 中的第 n 个素数.

我们也能得到一个关于 q 为一致的结果. 实际上, Page[157] 证明了: (a)$L(s,\chi)$ 在

$$t\geqslant 3,\quad \sigma>1-\frac{\alpha_2}{\log qt}$$

中没有零点; (b) 对于任何复特征 $\chi, L(s,\chi)$ 在 $\sigma\geqslant 1-\dfrac{\alpha_3}{\log q},|t|\leqslant 5$ 中没有零点;(c) $L(s,\chi)$ 在

$$\sigma\geqslant 1-\frac{\alpha_4}{\log q},\quad 0<t<5$$

中没有零点; (d) 设 $\xi\geqslant 2$, 在由以 $q(\leqslant\xi)$ 为模的实原特征所构成的全体 L- 函数中, 至多有一函数, 它有一实零点适合 $\sigma>1-\dfrac{\alpha_5}{\log \xi}$. 利用这些结果, 我们导得

$$\pi(x;q,l)=\frac{1}{\varphi(q)}\mathrm{li}\ x+O(x\mathrm{e}^{-c(\log\ x)^{\frac{1}{2}}})+O\left(\frac{x^{\sigma_1}}{\varphi(q)\log\ x}\right),$$

此处 σ_1 为模 q 的 L- 函数所具有的最大实零点, 而 c 为一正常数. Tatuzawa[158] 对此公式作了某种改进.

有没有可能把第二个误差项除去? 它的困难点在于有实特征的 L- 函数的实零点的分布情形. 以后在 C. L. Siegel[159] 关于二次型类数的 Gauss 问题的极为重要的工作中, 这个困难被克服了. 他证明了: 对于任何给定的 $\varepsilon>0$, 存在数 A, 使在 $\sigma>1-q^{-\varepsilon}$ 与 $q>A$ 中, 有

$$L(\sigma,\chi)\neq 0.$$

通过将 Page 与 Siegel 的结果的结合, Walfisz[160] 建立了下面的重要定理: 设 $q\geqslant 3$, 又 $q\leqslant(\log x)^h$ 而 $h\geqslant 1$，则有

$$\pi(x;q,l)=\frac{1}{\varphi(q)}\mathrm{li}\ x+O(x\mathrm{e}^{-c(\log\ x)^{\frac{1}{2}}}),\tag{85}$$

记号 O 中所含的常数与 q 无关.

虽然这个公式远优于 Page 的结果, 但在它的证明中, 还有一点不足之处. 因为 Siegel 的定理只是一个存在性定理, 我们无法通过有限的步骤来找出 (85) 中的显常数. 例如, 如果用 (85) 去证明Виноградов 的“三素数定理”, 我们就无法定出奇素数究竟需要大到怎样程度才能表成三个素数的和. 但是我们能够避开 Siegel 定理, 而用 Page 原来的工作, 来证明具有确定数值常数的“三素数定理”.

关于等差级数中的素数分布, 另一个有趣问题是为等差级数 $\equiv l(\bmod q)$ 中的最小素数 $p(q,l)$ 找一上界. Линник[161] 开辟了重要的一步. 他证明了: 这种素数一

定是 $O(q^c)$, c 为一绝对常数. 以后, Родосский[162] 简化了他的证明. S. Chowla[163] 猜测: 对于任何 $\varepsilon > 0$ 及对全体大 $q, \equiv l(\mathrm{mod}\ q)$ 的最小素数一定不大于 $q^{1+\varepsilon}$; Turán[164] 证明: 如果广义黎曼猜想成立, 那么 Chowla 的猜想对几乎全体模 q 的等差级数都正确. 另一方面, Erdös[165] 证明了: (a) 存在常数 $c_2 = c_2(c_1)$ 与无穷多个整数 q, 使

$$p(q,l) > (1+c_1)\varphi(q)\log q$$

对不少于 $c_2\varphi(q)$ 个 l 值成立; (b) 存在常数 $c_4 = c_4(c_3)$, 使

$$p(q,l) \leqslant c_3\varphi(q)\log q$$

对 $c_4\varphi(q)$ 个 l 值成立.

3.8 其他素数问题

设 $\pi_\nu(x;q,l)$ 为不大于 x 并且是 ν 个素数的乘积, 同时又是 $\equiv l(\mathrm{mod}\ q)$ 的整数的个数. Richert [166] 证明了:

$$\begin{aligned}\pi_\nu(x;q,l) =& \frac{1}{\varphi(q)}\sum_{0\leqslant m\leqslant \frac{1}{c}\sqrt{\log x}}\ \sum_{0\leqslant h\leqslant \nu-1} A_\nu(h,m,q)\int_2^x \frac{(\log\log u)^h}{(\log u)^{m+1}}\mathrm{d}u\\ &+ O(x\mathrm{e}^{-\frac{1}{c}\sqrt{\log x}}) + O\left(x^{1-\frac{1}{bq^\varepsilon}}\frac{\log^{\nu-1} q(\log\log x)^{\nu-1}}{\varphi(q)\log x}\right),\end{aligned}$$

这里的 b 为一与 ε 有关的数, $c(\geqslant 20)$ 为一常数, $A_\nu(h,m,q)$ 通过一个只与 h, m, q 及 ν 有关的级数而定义.

И. И. Пятецкий-Шапиро[167] 证明了: 对于 $1 \leqslant c < \dfrac{12}{11}$, 在序列 $[n^c]$ 中不大于 x 的素数个数与 $\dfrac{x^{\frac{1}{c}}}{\log x}$ 渐近相等.

Landau[168] 将素数分布理论方面的古典结果推广到任何代数数域.

设 k 为一 n 次代数数域, $\pi_k(x)$ 为有距 $\leqslant x$ 的素理想数的个数, 则有

$$\begin{aligned}&\pi_k(x) = \mathrm{li}\ x + O(x\mathrm{e}^{-\frac{\alpha}{\sqrt{n}}\sqrt{\log x}}),\\ &\vartheta_k(x) = \sum_{NP\leqslant x}\log N\mathfrak{p} = x + O(x\mathrm{e}^{-\frac{\alpha}{\sqrt{n}}\sqrt{\log x}}),\end{aligned}$$

此处 α 为一绝对常数, 又有

$$\pi_k(x) - \mathrm{li}\ x = \Omega_\pm \frac{\sqrt{x}}{\log x}\log\log\log x.$$

对于类中的理想数也有类似的结果.

3.9 素因子有某种特殊性质的整数的分布

命 $\Phi(x,y)$ 表示 $\leqslant x$ 且无素因子 $< y$ 的自然数的个数. Бухштаб[169] 证明了

$$\Phi(y^u,y)=w(u)\frac{y^u}{\log y}+O\left(\frac{y^u}{(\log^u y)^{\frac{3}{2}}}\right), \tag{86}$$

记号 O 中所含的常数与 u 无关, 并且

$$\left.\begin{aligned} w(u)&=\frac{1}{u}, \quad 1\leqslant u\leqslant 2,\\ (uw(u))'&=w(u-1), \quad u>2. \end{aligned}\right\} \tag{87}$$

命 $\psi(x,y)$ 表示 $\leqslant x$ 且无素因子 $> y$ 的自然数的个数, 则有

$$\psi(y^u,y)=\rho(u)y^u+O\left(\frac{y^u}{(\log y)^{\frac{1}{2}}}\right), \tag{88}$$

此处

$$\left.\begin{aligned} \rho(u)&=1, \quad 0<u\leqslant 1,\\ u\rho'(u)&=-\rho(u-1), \quad (u>1). \end{aligned}\right\}^{170),171)} \tag{89}$$

函数

$$f(s)=\int_0^\infty \mathrm{e}^{-su}\mathrm{d}w(u+1)$$

满足下之微分方程:

$$f'(s)+(s^{-1}(\mathrm{e}^{-s}-1)-1)f(s)=s^{-1}(1-\mathrm{e}^{-s}).$$

解此方程, 并因

$$\lim_{s=\infty}f(s)=0,$$

故得

$$f(s)=-1-s\mathrm{e}^s+\mathrm{e}^{-\gamma+s+\int_0^s t^{-1}(1-\mathrm{e}^{-t})\mathrm{d}t}.$$

命 $s\to 0$, 则有

$$-1+\mathrm{e}^{-\gamma}=\lim_{s\to 0}f(s)=\lim_{s\to 0}\int_0^\infty \mathrm{e}^{-us}\mathrm{d}w(u+1)=\int_0^\infty \mathrm{d}w(u+1)=w(\infty)-w(1),$$

也即

$$\lim_{u\to\infty}w(u)=\mathrm{e}^{-\gamma}. \tag{90}$$

因为

$$w(u) - \mathrm{e}^{-\gamma} = -\int_u^{\infty} w'(t)\mathrm{d}t$$

及

$$w'(u) = -\frac{1}{u}\int_{u-1}^{u} w'(t)\mathrm{d}t,$$

故由下面的初等引理, 我们得到

$$w'(u) < \mathrm{e}^{-u(\log u+\log\ \log u-\frac{\log\ \log u}{\log u}+O(\frac{1}{\log u}))}$$

及

$$|w(u) - \mathrm{e}^{-\gamma}| < \mathrm{e}^{-u(\log u+\log\ \log u-\frac{\log\ \log u}{\log u}+O(\frac{1}{\log u}))}. \tag{91}$$

引　设 $F(u)$ 为在 $u>0$ 时定义的一个正值函数, 又对充分大的 $u, F(u)$ 适合不等式

$$F(u) \leqslant \frac{1}{u}\int_0^1 F(u-1+\vartheta)\mathrm{d}\vartheta,$$

则有

$$F(u) \leqslant \mathrm{e}^{-u(\log u+\log\ \log u-1+\frac{\log\ \log u}{\log u}+O(\frac{1}{\log u}))}.$$

类似地, 我们能够证明

$$\rho(u) = \mathrm{e}^{-u(\log u+\log\ \log u-1+\frac{\log\ \log u}{\log u})+O(\frac{u}{\log u})}\text{[172),173),174),175)]}. \tag{92}$$

De Bruijn 引进了函数 Λ:

$$\Lambda(y^u, y) = y^u\int_0^{\infty}\rho\left(\frac{u\log y-\log t}{\log y}\right)\mathrm{d}\frac{[t]}{t},$$

并以此代替 (88) 中的 $y^u\rho(u)$, 从而证得了

$$\psi(y^u, y) = \Lambda(y^u, y) + O(u^2y^uR(y))\text{[176)]}, \tag{93}$$

式中 $R(y)$ 的阶大体上为 $\dfrac{|\pi(y)-\mathrm{li}\ y|}{y}$.

本节的结果可以推广到一个给定的等差级数中.

第 4 章 Waring 问题

4.1 解析方法的引进

设 k 与 N 都是自然数, 命 $P=[N^{\frac{1}{k}}]$, 又命

$$T(\alpha)=\sum_{x=1}^{P}\mathrm{e}^{2\pi\mathrm{i}\alpha x^k},$$

则

$$r_s(N)=\int_0^1 (T(\alpha))^s\mathrm{e}^{-2\pi\mathrm{i}N\alpha}\mathrm{d}\alpha=\int_{-\frac{1}{\tau}}^{1-\frac{1}{\tau}}(T(\alpha))^s\mathrm{e}^{-2\pi\mathrm{i}N\alpha}\mathrm{d}\alpha \tag{94}$$

就是不定方程

$$x_1^k+x_2^k+\cdots+x_s^k=N,\quad x_i\geqslant 1 \tag{95}$$

的解数, 此处 $\tau=2kP^{k-1}$.

用 $\mathfrak{M}_{h,q}$ 表示区间

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{1}{q\tau},\quad (h,q)=1,\ q\leqslant P^{\beta},$$

此处 $\frac{1}{4}\leqslant\beta\leqslant 1-\frac{1}{k}$. 今往估计 $\mathfrak{M}_{h,q}$ 上的 $T(\alpha)$. 置 $x=qy+r$ 及 $\alpha=\frac{h}{q}+\vartheta$, 则有

$$T(\alpha)=\sum_{r=1}^{q}\mathrm{e}^{2\pi\mathrm{i}hr^k/q}\sum_{0\leqslant qy+r\leqslant P}\mathrm{e}^{2\pi\mathrm{i}(qy+r)^k\vartheta}.$$

命 $f(y)=\vartheta(qy+r)^k$, 因为

$$|f'(y)|=|k\vartheta(qy+r)^{k-1}q|<\frac{kP^{k-1}q}{2kq\ P^{k-1}}=\frac{1}{2},$$

故按 §8 引理 1 可得

$$\begin{aligned}T(\alpha)=&\sum_{r=1}^{q}\mathrm{e}^{2\pi\mathrm{i}hr^k/q}\int_{0<qt+r\leqslant p}\mathrm{e}^{2\pi\mathrm{i}(qs+r)^k\vartheta}\,\mathrm{d}t+O(q)\\=&\frac{1}{q}\sum_{r=1}^{q}\mathrm{e}^{2\pi\mathrm{i}hr^k/q}\int_0^P\mathrm{e}^{2\pi\mathrm{i}x^k\vartheta}\,\mathrm{d}x+O(q).\end{aligned}$$

借助于下面两个估计：

$$\sum_{r=1}^{q} \mathrm{e}^{2\pi \mathrm{i} h r^k/q} = O(q^{1-\frac{1}{k}}), \quad \int_0^P \mathrm{e}^{2\pi \mathrm{i} x^k \vartheta} \mathrm{d}x = O(\min(P, |\vartheta|^{-\frac{1}{k}})),$$

我们得出

$$\begin{aligned}\int_{\mathfrak{M}_{h,q}} (T(\alpha))^s \mathrm{e}^{-2\pi \mathrm{i} \alpha N} \mathrm{d}\alpha =& \frac{1}{q^s}\Big(\sum_{r=1}^{q} \mathrm{e}^{2\pi \mathrm{i} h r^k/q}\Big)^s \mathrm{e}^{-2\pi \mathrm{i} h N/q} \\ & \times \int_{-\infty}^{+\infty} \Big(\int_0^P \mathrm{e}^{2\pi \mathrm{i} x^k \vartheta} \mathrm{d}x\Big)^s \mathrm{e}^{-2\pi \mathrm{i} N \vartheta} d\vartheta \\ & + O\Big(\frac{P^{s-k-1}}{q}\Big) + O\Big(\frac{P^{s-k-\frac{1}{k}}}{q^{2+\frac{1}{k}}}\Big).\end{aligned}$$

最后, 对于 $s \geqslant 2k+1$, 我们得到

$$\sum_{\mathfrak{M}_{h,q}} \int_{\mathfrak{M}_{h,q}} (T(\alpha))^s \mathrm{e}^{-2\pi \mathrm{i} \alpha N} \mathrm{d}\alpha = \mathfrak{S}(N) N^{\frac{s}{k}-1} \frac{\Gamma^s\Big(1+\dfrac{1}{k}\Big)}{\Gamma\Big(\dfrac{s}{k}\Big)} + O(P^{s-k-\frac{1}{k}}),$$

此处

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{\substack{h=1 \\ (h,q)=1}}^{q} \Big(\frac{1}{q} \sum_{x=1}^{q} \mathrm{e}^{2\pi \mathrm{i} h x^k/q}\Big)^s \mathrm{e}^{-2\pi \mathrm{i} N h/q}.$$

对于 $s \geqslant 4k$, 我们能够证明

$$\mathfrak{S}(N) \gg 1.$$

于是问题化为去估计积分 (94) 在 E 上的部分, E 是不属于任何 $\mathfrak{M}_{h,q}$ 的点的集合. 如果它的阶等于 $o(P^{s-k})$, 则对大 N, 将有 $r_s(N) > 0$.

积分的剩余部分的处理依赖于下面两个估计：由第二章, §7得出的

$$\max_{\alpha \in E} |T(\alpha)| \ll P^{1-2^{1-k}+\varepsilon} \tag{96}$$

及

$$\int_0^1 |T(\alpha)|^{2^k} \mathrm{d}\alpha \ll P^{2^k-k+\varepsilon}. \tag{97}$$

于是对于 $s > 2^k$, 可有 [177)]

$$r_s(N) = \int_0^1 (T(\alpha))^s \mathrm{e}^{-2\pi \mathrm{i} N \alpha} \mathrm{d}\alpha \sim \mathfrak{S}(N) N^{\frac{s}{k}-1} \frac{\Gamma^s\Big(1+\dfrac{1}{k}\Big)}{\Gamma\Big(\dfrac{s}{k}\Big)}. \tag{98}$$

Виноградов[27] 用另外两个估计代替 (96) 及 (97), 它们是

$$\max_{\alpha\in E}|T(\alpha)| \ll P^{1-\frac{1}{2k^2(2\log k+\log\log k+3)}+\varepsilon}, \tag{99}$$

以及对 $t \geqslant \frac{1}{4}k(k+1)+lk, 0 \leqslant l \leqslant c_1(k)$ 成立的

$$\int_0^1 |T(\alpha)|^{2t}\mathrm{d}\alpha \ll P^{2t-k+\delta}(\log P)^{2l}, \tag{100}$$

此处

$$\delta = \frac{1}{2}\Big(1-\frac{1}{k}\Big)^l k(k+1)$$

(它由§9定理 1 导出). 于是对于

$$s \geqslant 2k^2(2\log k+\log\log k+2.5)^{178)}$$

与 $k>10$, (98) 式成立.

Hardy-Littlewood 会经猜测

$$\sum_{n=1}^{N} r_k^2(n) = O(N^{1+\varepsilon})$$

成立, 或者与它等价的有

$$\int_0^1 |T(\alpha)|^{2k}\mathrm{d}\alpha \ll P^{k+\varepsilon}.$$

假如这个猜测正确, 那么容易看到, 上面的渐近公式对于 $s \geqslant 2k+1$ 成立. 但除在 $k=2$ 时外, 这个猜测之为正确或为错误, 至今还未能够确定. 由此猜测. 我们立刻推得: 除在 $k=2^m$ 而 $m>1$ 时外, 都有

$$G(k) \leqslant 2k+1,$$

而在这些例外情形中,$G(k)=4k$. $G(k)$ 的意义将在§26中给出.

假如

$$r_k(n) = O(n^{\varepsilon}),$$

则 Hardy-Littlewood 的猜测就能成立. 但另一方面, Erdös[179], Chowla 与 Pillai[180] 证明了

$$r_k(n) = \Omega(\mathrm{e}^{c\log n/\log\log n}).$$

对于 $k=3$ 的情形. Mahler[181] 证明

$$x^3+y^3+z^3 = n^{12}$$

的解数 $\gg n$.

4.2　$G(k)$ 的上界

命 $G(k)$ 为使

$$x_1^k+\cdots+x_s^k=N,\quad x_\nu\geqslant 0 \tag{101}$$

对全体充分大的 N 都有整数解 x_ν 的最小整数 s. 上节的结果不仅告诉我们

$$G(k)\leqslant\begin{cases}2^k+1, & k\leqslant 10,\\ 2k^2(2\log k+\log\log k+2.5), & k>10,\end{cases}$$

并且还给出了 (101) 的解数的渐近公式. 如果我们无意保住此渐近公式, 我们便能得到 $G(k)$ 的一个更好的上界. 下述方法属于Виноградов, 它以下面的引理作为出发点.

引 1(Hardy-Littlewood)　命

$$P_1=\left[\frac{1}{4}P\right],\ P_2=\left[\frac{1}{2}P_1^{1-\frac{1}{k}}\right],\ \cdots,\ P_m=\left[\frac{1}{2}P_{m-1}^{1-\frac{1}{k}}\right],$$

又命 $\xi_i(i=1,2,\cdots,m)$ 经过区间

$$P_i\leqslant\xi_i<2P_i$$

中的整数, 则对固定的 m 与对充分大的 P, 数

$$u=\xi_1^k+\cdots+\xi_m^k$$

各各不同, 并且都在 $\left(\frac{1}{5}P\right)^k$ 与 $\left(\frac{1}{2}P\right)^k$ 之间. 又设 $P_m\leqslant\xi'_m<2P_m$, 则对任何 $\varepsilon>0$ 及对给定的 v, 方程

$$v=\xi_1^k+\cdots+\xi_m^k+{\xi'}_m^k$$

的解数等于 $O(v^\varepsilon)$. 这种 v 的个数 $\gtrless P^{k-(k-2)(1-\frac{1}{k})^{m-1}}$.

引理的第一部分由下之事实, 即由

$$(\xi_1+1)^k-\xi_1^k\geqslant k\xi_1^{k-1}\geqslant kP_1^{k-1}>(2P_2)^k+\cdots+(2P_m)^k>\xi_2^k+\cdots+\xi_m^k$$

导出. 引理的第二部分还需要另外一个结果, 即 $\xi_m^k+{\xi'}_m^k=w$ 的解数等于 $O(w^\varepsilon)$.

命

$$T_{i-1}(\alpha)=\sum_{\xi_i}\mathrm{e}^{2\pi\mathrm{i}\xi_i^k\alpha},$$

$$Q(\alpha)=T_1(\alpha)\cdots T_m(\alpha)T_{m+1}^2(\alpha)$$

及

$$R(\alpha) = T_0(\alpha)Q(\alpha).$$

引理告诉我们,

$$\int_0^1 |R(\alpha)|^2 \mathrm{d}\alpha \ll R(0)P^{\varepsilon}.$$

命

$$b = \begin{cases} 2k^2(2\log k + \log\log k + 3,) & k > 12, \\ 2^{k-1}, & k \leqslant 12 \end{cases} \tag{102}$$

及

$$m = \left[\frac{\log\frac{1}{2}b + \log\frac{(k-2)}{(k-\frac{1}{2})}}{-\log\left(1 - \frac{1}{k}\right)} \right], \tag{103}$$

则在 E 上可有

$$\begin{aligned}\int_E |T_0^{2k-1}(\alpha)R^2(\alpha)|\mathrm{d}\alpha &\ll \max_{\alpha\in E} |T_0(\alpha)|^{2k-1} \int_0^1 |R(\alpha)|^2 \mathrm{d}\alpha \\ &\ll P^{(1-\frac{1}{b})(2k-1)+\varepsilon}R(0) = o(P^{k+1}Q^2(0)),\end{aligned}$$

这是因为

$$(k-2)\left(1 - \frac{1}{k}\right)^{m+1} < \frac{2k-1}{b}$$

的原故. 又不难证明

$$\sum_{\mathfrak{M}_{h,q}} \int_{\mathfrak{M}_{h,q}} T_0^{2k-1}(\alpha)R^2(\alpha)\mathrm{e}^{-2\pi\mathrm{i}\alpha N}\mathrm{d}\alpha \gg P^{k+1}Q^2(0).$$

于是因为 $m \sim 2k\log k$, 所以我们建立了

$$G(k) \leqslant 2k + 2m + 5 \sim 4k\log k.$$

这个结果又被Виноградов[27] 进一步改进为：对于 $k \geqslant 3$, 有

$$G(k) < 3k(\log k + 9).$$

证明依赖于下面的

引 2　设

$$U(\alpha) = \sum_p \sum_{u_0} \mathrm{e}^{2\pi\mathrm{i}\alpha_p{}^k u_0},$$

此处 u_0 经过引理 1 中给出的整数集合, 但以 $[P^{\frac{1}{2}}]$ 代替 P 与以 m_0 代替 m, 又 p 经过区间 $\frac{1}{2}[P^{\frac{1}{2}}] \leqslant p \leqslant [P^{\frac{1}{2}}]$ 中的全体素数. 于是当 $\alpha \in E$ 时, 有

$$U(\alpha) \ll U(0)P^{-\frac{1}{8}+\frac{k}{4}(1-\frac{1}{k})^{m_0}+\varepsilon}.$$

我们选取 m_0 与 m 为使

$$k\Big(1-\frac{1}{k}\Big)^{m_0-1} < \frac{1}{6} \quad 与\ k\Big(1-\frac{1}{k}\Big)^{m} < \frac{1}{12}$$

成立的最小整数, 亦即

$$m_0 = \left[\frac{\log 6k}{-\log\Big(1-\dfrac{1}{k}\Big)}+2\right] \quad 与\ m = \left[\frac{\log 2k}{-\log\Big(1-\dfrac{1}{k}\Big)}+1\right],$$

则因

$$|T(\alpha)| = \left|\sum_{x=1}^{P} \mathrm{e}^{2\pi\mathrm{i}x^k a}\right| \leqslant P,$$

故得

$$\begin{aligned}\int_E T(\alpha)^{2k+1}R^2(\alpha)U(\alpha)\mathrm{d}\alpha \ll& P^{2k+1}\max_{\alpha\in E}|U(\alpha)|\int_0^1|R(\alpha)|^2\mathrm{d}\alpha\\ \ll& P^{2k+1}U(0)P^{-\frac{1}{8}+\frac{1}{24}(1-\frac{1}{k})+\varepsilon}R(0)\\ \ll& P^{2k+1}U(0)R^2(0)P^{-k-\frac{1}{24k}}.\end{aligned}$$

于是我们能够证明: 当 $P\to\infty$ 时, 有

$$\int_0^1 T(\alpha)^{2k+1}R^2(\alpha)U(\alpha)\mathrm{e}^{-2\pi\mathrm{i}\alpha N}\mathrm{d}\alpha \sim cT(0)^{k+1}R^2(0)U(0)$$

与 $c>0$. 由此得出: 对于 $k\geqslant 3$, 有

$$G(k) \leqslant 2k+1+m_0+2m < 3k(\log k+3).$$

Davenport[28)] 改进了引 1, 从而能够证明: $G(4)=16$(一个变化了的数: $G^*(4)\leqslant 14$), $G(5)\leqslant 23$, $G(6)\leqslant 36$, $G(7)\leqslant 52$, $G(8)\leqslant 73$).

Линиик[29)] 证明了: $G(3)\leqslant 7$. (另有一个简单证明, 请见 Watson [182)]).

我们可以通过两个不同的方法来证明 $G(k)$ 的下界 $\geqslant k+1$:

a) 能够表成

$$x_1^k+\cdots+x_k^k, \quad x_\nu \geqslant 0$$

形状的 $n(\leqslant N)$ 的个数少于满足条件

$$0 \leqslant x_1 \leqslant x_2 \leqslant \cdots \leqslant x_k \leqslant [N^{\frac{1}{k}}]$$

的 $x_1, \cdots, x_k$ 的组数. 显然, 对于充分大的 N, 后者 $< \frac{2}{3}N$.

b) 关于同余式的考虑.

直到 1909 年为止, 这个由 Waring[4] 提出的问题只在不多的数值结果中显示出微小的苗头. 1909 年, Hilbert[5] 证明了：对于每一 $k, G(k)$ 都存在. 他先用一个 25 重的重积分证明了下面的事实: 对于每一 k, 都存在一个有五个变元 $x_1, \cdots, x_5$ 的形状如

$$(x_1^2 + \cdots + x_5^2)^k = \sum_h r_h(a_{1h}x_1 + \cdots + a_{5h}x_5)^{2k}$$

的恒等式, 其中 a_{ih} 都是整数, 而 r_h 则是正有理数. 这是在证明关于 $k = 2^m (m = 1, 2, \cdots)$ 的 Waring 定理过程中的一个步骤. 任意指数的情形能够由此通过一个冗长的研究而得出.

虽然 Hilbert 的证明被很多数学家 [183] 所简化, 但由此方法得到的 $G(k)$ 仍然过大.

Hardy 与 Littlewood 在 1920—1928 年出版的总标题为 “partitio numerorum” 的一系列工作中, 展开了一个重要的研究 Waring 问题的解析方法. 但关于 $G(k)$ 上界的最重要的改进, 还是Виноградов 得到的. 他引进了数论中的一个强有力的方法, 即三角和方法.

4.3 Waring 问题的各种推广

设 $f(x)$ 为一 k 次整值多项式. 前述的大多数结果, 除开 $G(3) \leqslant 7$与$G(k) < k(3\log k + 9)$ 外, 都能推广到多项式的情形. 华罗庚 [98],[184] 克服了其中的主要困难. 例如, 我们能够证明：对于 $k \leqslant 10$而$s \geqslant 2^k + 1$, 以及对于 $k > 10$而$s \geqslant 2k^2(2\log k + \log\log k + 2.5)$, 关于

$$N = f(x_1) + \cdots + f(x_s) \tag{104}$$

的解数, 有一渐近公式. 又

$$N = f_1(x_1) + \cdots + f_s(x_s)$$

的问题 [177],[185] 也如此.

设

$$f(x) = ak\binom{x}{k} + a_{k-1}\binom{x}{k-1} + \cdots + a_1\binom{x}{1}$$

及

$$(a_k,\ a_{k-1},\ \cdots,\ a_1) = 1,$$

此处 $\binom{x}{r} = \dfrac{x(x-1)\cdots(x-r+1)}{r!}$. 我们定义 $G(f)$ 为使方程 (104) 对全体充分大的 N 都可解的最小整数 s. 华罗庚 [186] 证明了

$$G(k\text{次多项式}) \leqslant (k-1)2^{k+1}$$

与 [187]

$$G(3\text{次多项式}) \leqslant 8.$$

Нечаев[188] 证明

$$G\left(\binom{x}{k}\right) < 4k\log k + 8k\log\log k.$$

又华罗庚 [186] 指出

$$\max_{f(x)} G(f) \geqslant 2^k - 1,$$

这里的 $f(x)$ 经过全体 $k(\geqslant 5)$ 次整值多项式.

命 $G^*(f(x))$ 表示使

$$f(x_1) + \cdots + f(x_s) = N$$

在

$$f(x_1) + \cdots + f(x_s) \equiv N \pmod q$$

对任何 q 都可解时为可解的最小整数 s, 则有 [189]

$$G^*(f(x)) \leqslant 2m + 2k + 5 \sim 4k\log k,$$

m 的定义见第 4 章 §26 中的 (102) 与 (103). 又依靠 Davenport 引理的帮助, 还能得到一些特殊结果, 例如,

$$G^*(\text{四次多项式}) \leqslant 14,$$
$$G^*(\text{五次多项式}) \leqslant 23.$$

Roth[190] 证明: 每一充分大的整数都能表成 $x_1^2 + x_2^3 + \cdots + x_{50}^{51}$ 的形成, $x_i(i = 1, 2, \cdots, 50)$ 都是正整数. 他还证明: 几乎全体正整数 n 都能表成

$$x_1^2 + x_2^3 + x_3^4 + x_4^5$$

的形状.

Wright[191] 在变量上添加了阶的条件, 他证明了: 设 $\lambda_1, \cdots, \lambda_s$ 都是正数, 并且 $\sum_{\nu=1}^{s} \lambda_\nu = 1$, 又设 $k \geqslant 3$, 而

$$s \geqslant (k-2)2^{k-1} + 5,$$

则每一充分大的整数 n 都能表成 s 个正的 k 次乘幂的和, 如

$$n = m_1^k + \cdots + m_s^k,$$

并且这些 m 适合

$$|\lambda_i n - m_i^k| = O(n^{1-\beta}), \quad i = 1, 2, \cdots, s.$$

此处 $0 < \beta < \alpha$, 而 α 为 k 与 s 的某一函数. 例如, 若 $k = 3$ 与 $s = 9$, 则 $\alpha = \dfrac{1}{51}$. 如果用Виноградов的方法, 这个结果肯定还能改进.

对于 $n \not\equiv 0 \pmod 8$ 的情形, Auluck 与 Chowla[192] 证明: n 能够表成

$$n = m_1^2 + \cdots + m_4^2$$

的形状, 此处

$$\frac{n}{4} - m_i^2 = O(n^{\frac{3}{4}}).$$

命 $c > 1$, 但非整数. Cerад[193] 曾经研究用形如

$$x_1^c + x_2^c + \cdots + x_s^c$$

的表示式来近似表示数的问题, 这里的 x_i 都是正整数. Cerад[193] 证明了: 存在 $s_0(c)$, 使当 $s \geqslant s_0(c)$ 时, 不等式

$$\left| \sum_{i=1}^{s} x_i^c - N \right| < \Delta_N$$

为可解, 这里的 Δ_N 在 N 趋向无穷进趋于零.

另外还有一些问题, 它们在某些方面与 Waring 问题相似. 例如, 定出 s 的下界 $s_0(k)$, 使不等式

$$\left| \sum_{i=1}^{s} \lambda_i x_i^k \right| < \varepsilon \tag{105}$$

对任何 $\varepsilon > 0$ 与 $s \geqslant s_0(k)$ 都有正整数解 x_i. 显然, 这些 λ 不能有相同的符号. Chowla[194] 证明: 如果比数 $\lambda_s/\lambda_t (s \neq t)$ 都是无理数, 则 $s_0(2) \leqslant 9$.

利用 Hardy-Littlewood 方法的一个变形, Davenport 与 Heilbronn[195] 证明了: 如果至少有一比数 $\lambda_s/\lambda_t (s \neq t)$ 为无理数, 则有 $s_0(2) \leqslant 5$. 在此同一条件下,

Davenport 与 Roth[196] 讨论了 $k=3$ 的情形, 他们证明了 $s_0(3)\leqslant 8$. 另外他们用Виноградов 处理 Waring 问题的方法证明了：存在绝对常数 c, 使对 $k\geqslant 12$, 有

$$s_0(k)\leqslant ck\log k.$$

关于下述问题的研究, 请见 Oppenheim[197]. 这个问题是, 确定 s 的下界 s_0, 使不等式

$$0<f(x_1,\cdots,x_s)<\varepsilon$$

对任何 $\varepsilon>0$ 都有整数解 x_i, 此处 f 为一具实系数的不定二次型.

4.4　$g(k)$ 的上界

用 $g(k)$ 表示使

$$N=x_1^k+\cdots+x_s^k,\quad x_i\geqslant 0$$

对全体整数 $N\geqslant 0$ 都可解的最小整数 s. 命 $q=\left[\left(\frac{3}{2}\right)^k\right]$, 数

$$n=2^kq-1<3^k$$

只可能用 1^k 与 2^k 表出. 因为

$$n=(q-1)2^k+(2^k-1)\cdot 1^k,$$

故在 n 的表示中正巧需要

$$q-1+2^k-1=2^k+q-2$$

个 k 次乘幂. 因此

$$g(k)\geqslant 2^k+q-2.$$

对于 $g(k)$, Виноградов 的方法也能导致非常出色的结果. Dickson[30] 与 Pillai[31] 相互独立地得到了有关 $g(k)$ 问题的几乎最后的解决. 这个解的第一部分也是最深刻的部分, 有赖于Виноградов 方法的应用. 第二部分则依赖于一个称为“上升法”的方法. 它的最后结果是：对于 $k>6$ 且使

$$\left(\frac{3}{2}\right)^k-\left[\left(\frac{3}{2}\right)^k\right]\leqslant 1-\left(\frac{1}{2}\right)^k\left\{\left[\left(\frac{3}{2}\right)^k\right]+3\right\}\tag{106}$$

成立的全体 k, 都有

$$g(k)=2^k+\left[\left(\frac{3}{2}\right)^k\right]-2.\tag{107}$$

这一条件在 $4 \leqslant k \leqslant 400$ 时成立, 它也可能对全体 $k > 3$ 都成立. 以后, Pillai[31] 证明: 对于 $k = 6$, (107) 也真确, 亦即 $g(6) = 73$. 于是现在除了 $k = 4$ 及 $k = 5$, 以及 (106) 是否成立尚未获得确定的任何 $k > 3$, 问题的解就完整了. $g(3) = 9$ 很早以前已被 Wieferich 所证得. 对于 $k = 4$ 及 $k = 5$, 已知的最佳的不等式是

$$19 \leqslant g(4) \leqslant 35,\ 37 \leqslant g(5) \leqslant 54,$$

其中的上界都是 Dickson[198] 给出的.

Нечаев[189] 证明了 $g\left(\binom{x}{k}\right) < 6k \log k + 8k \log \log k$.

设 $u = u_i$ 为一形如 x^m 的数, 此处 $m \geqslant n$. Pillai[199] 证明: 对于全体 $n \geqslant 32$, 使方程 $N = u_1 + \cdots + u_s$ 对于任何 N 都为可解的 s 的最小值都等于

$$2^n + \left[\frac{1}{\log 2}\log\left[\left(\frac{3}{2}\right)^n\right]\right] - 1.$$

4.5 齐次问题

用 $N(k)$ 表示使方程组

$$\left.\begin{array}{c} x_1 + \cdots + x_t = y_1 + \cdots + y_t \\ \cdots\cdots \\ x_1^k + \cdots + x_t^k = y_1^k + \cdots + y_t^k \end{array}\right\} \tag{108}$$

在下述的意义下为可解的最小整数 t : $x_1, \cdots, x_t, y_1, \cdots, y_t$ 都是正整数, 但 $y_1, \cdots, y_t$ 不能是 $x_1, \cdots, x_t$ 的重新排列. 又用 $M(k)$ 表示使方程组 (108) 为可解且使

$$x_1^{k+1} + \cdots + x_t^{k+1} \neq y_1^{k+1} + \cdots + y_t^{k+1}$$

成立的最小的 t, 显然有

$$k + 1 \leqslant N(k) \leqslant M(k).$$

用初等方法可以证明 $N(k) \leqslant \frac{1}{2}k(k+1) + 1$. Wright[200] 证明了

$$N(k) \leqslant \begin{cases} \frac{1}{2}(k^2+3), & \text{假如} 2 \nmid k, \\ \frac{1}{2}(k^2+4), & \text{假如} 2 | k. \end{cases}$$

又华罗庚[201] 证明了

$$M(k) \leqslant (k+1)\left(\left[\frac{\log \frac{1}{2}(k+2)}{\log\left(1+\frac{1}{k}\right)}\right] + 1\right),$$

它是下述的由华罗庚 [202] 证明的更一般性定理的直接推论.

定理　设 $i \geqslant (k+1)\left(\left[\dfrac{\log\frac{1}{2}(k+2)}{\log\left(1+\frac{1}{k}\right)}\right]+1\right)$. 对于任何给定的 s, 必存在 $N_1, \cdots, N_k$; $M_1, \cdots, M_s$(当 $t_1 \neq t_2$ 时, $M_{t_1} \neq M_{t_2}$), 使下面 s 组不定方程

$$R_t(1 \leqslant t \leqslant s)\begin{cases}\displaystyle\sum_{i=1}^{i} x_{it}^h = N_h, \quad 1 \leqslant h \leqslant k,\\ \displaystyle\sum_{i=1}^{i} x_{it}^{k+1} = M_t\end{cases}$$

都为可解.

华罗庚 [26][82] 还证明了下面的

定理　设 $k \geqslant 2$, 又 t_0 为由下表定义的一个与 k 有关的整数:

k	2	3	4	5	6	7	8	9	10	$\geqslant 11$
t_0	3	8	23	55	120	207	336	540	885	$[k^2(3\log k + \log\log k + 4)]$

用 $r_t(P)$ 表示在

$$1 \leqslant x_i,\ y_i \leqslant P$$

的限制下不定方程组 (108) 的解数, 则对 $t > t_0$ 有

$$\lim_{P\to\infty} P^{\frac{1}{2}k(k+1)-2t} r_t(P) = \vartheta_0 \mathfrak{S},$$

此处

$$\vartheta_0 = \int_{-\infty}^{+\infty}\cdots\int_{-\infty}^{+\infty}\left|\int_0^1 \mathrm{e}^{2\pi\mathrm{i}(\beta_k x^k+\cdots+\beta_1 x)}\mathrm{d}x\right|^{2t}\mathrm{d}\beta_k\cdots\mathrm{d}\beta_1$$

而

$$\mathfrak{S} = \sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}\sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1}\cdots\sum_{\substack{h_k=1\\(h_k,q_k)=1}}^{q_k}\left|q_1^{-1}\cdots q_k^{-1}\sum_{x=1}^{q_1\cdots q_k}\mathrm{e}^{2\pi\mathrm{i}\left(\frac{h_k}{q_k}xk+\cdots+\frac{h_1}{q_1}x\right)}\right|^{2t}.$$

定理的证明主要基于Виноградов 的方法与华罗庚 [98] 引进的估计完整指数和的一个新方法.

设 $0 < i < j < \cdots < k$ 为 g 个整数, 又 $0 < N_i < N_j < \cdots < N_k$ 为给定的一些整数. 命 $N_k = P^k$(P 是实数). Марджанишвили[203] 曾经研究过在 N_i 充分大时,

不定方程组

$$\left.\begin{array}{c} x_1^i + x_2^i + \cdots + x_s^i = N_i \\ x_1^j + x_2^j + \cdots + x_s^j = N_j \\ \cdots\cdots \\ x_1^k + x_2^k + \cdots + x_s^k = N_k \end{array}\right\} \tag{109}$$

是否整数解的问题. 他证明了下面的

定理　设 $N_i = h_i P^i$, $N_j = h_j P^j$, $\cdots$, 又设 $k \geqslant 12$, $r = [2k \log 10kg + k\log\log 20kg] + 1$, $f > 3kg$ 为给定的常数. 如果存在常数 $\varepsilon > 0$, 使对 $s = f$, 方程组

$$\left.\begin{array}{c} \xi_1^i + \xi_2^i + \cdots + \xi_s^i = h_i \\ \xi_1^j + \xi_2^j + \cdots + \xi_s^j = h_j \\ \cdots\cdots \\ \xi_1^k + \xi_2^k + \cdots + \xi_s^k = h_k \end{array}\right\}$$

有适合

$$\xi_n \geqslant \varepsilon > 0, \quad n = 1, 2, \cdots, f$$

及

$$|\Delta| \geqslant \varepsilon$$

的实数解 $\xi_1, \cdots, \xi_f$, 此处

$$\Delta = \begin{vmatrix} x_1^{i-1}, & \cdots, & \xi_g^{i-1} \\ \vdots & & \vdots \\ \xi_1^{k-1}, & \cdots, & \xi_g^{k-1} \end{vmatrix},$$

则对具有 $s = f + 2gr$ 的方程组 (109), 它的正整数解 $x_1, \cdots, x_s$ 的解数 $I(N_i, \cdots, N_k; i, \cdots, k; s)$ 适合下面的不等式:

$$\begin{aligned} I > & c(i, \cdots, k; f, g, \varepsilon) N_k^{\frac{f}{k} + 2g(1-(1-\frac{1}{k})^r) - \frac{1}{k}(i+\cdots+k)} \mathfrak{S}(N_i, \cdots, N_k; s) \\ & + O(N_k^{\frac{f}{k} + 2g(1-(1-\frac{1}{k})^r) - \frac{1}{k}(i+\cdots+k) - \frac{w}{k}}), \end{aligned}$$

此处 c 与 w 为某两个正常数, 而 $\mathfrak{S}$ 就是所谓奇异级数.

关于 $\mathfrak{S}$ 为正的性质, 已在Марджанишвили的工作中探讨过.

第 5 章　Гольдбах 问 题

5.1　Виноградов 定理

用 $r(N)$ 表示将一奇数 N 表成三个素数之和的表法种数, 则有

$$r(N) = \int_0^1 (S(\alpha))^3 \mathrm{e}^{-2\pi \mathrm{i} N\alpha} \mathrm{d}\alpha,$$

此处

$$S(\alpha) = \sum_{p \leqslant N} \mathrm{e}^{2\pi \mathrm{i}\alpha p},$$

p 经过 $\leqslant N$ 的全体素数.

将积分区间移至 $\left(-\dfrac{1}{\tau},\ 1-\dfrac{1}{\tau}\right)$, 此处 $\tau = NL^{-h}$, 而 $L = \log N$, h 为一 $\geqslant 16$ 的正整数. 用 $\mathfrak{M}_{h,q}$ 表示区间

$$\alpha = \frac{a}{q} + \beta, \quad |\beta| \leqslant \frac{1}{\tau}, \quad 1 \leqslant q \leqslant L^h, \quad (a,q) = 1.$$

这些小区间互不重迭. 区间的剩余部分用 E 表示之.

在 $\mathfrak{M}_{h,q}$ 上可有

$$\begin{aligned}
\sum_{p \leqslant N} \mathrm{e}^{2\pi \mathrm{i} a p} &= \sum_{p \leqslant N} \mathrm{e}^{2\pi \mathrm{i}(\frac{a}{q}+\beta)p} \\
&= \sum_{\substack{r=1 \\ (r,q)=1}}^{q} \mathrm{e}^{2\pi \mathrm{i}\frac{ar}{q}} \sum_{n \leqslant N} \mathrm{e}^{2\pi \mathrm{i}\beta n} (\pi(n;q,r) - \pi(n-1;q,r)) + O(q) \\
&= \sum_{\substack{r=1 \\ (r,q)=1}}^{q} \mathrm{e}^{2\pi \mathrm{i}\frac{ar}{q}} \left(\sum_{n \leqslant N-1} \pi(n;q,r)(\mathrm{e}^{2\pi \mathrm{i}\beta n} - \mathrm{e}^{2\pi \mathrm{i}\beta(n+1)}) \right. \\
&\qquad \left. + \pi(N;q,r)\mathrm{e}^{2\pi \mathrm{i}\beta N} \right) + O(q).
\end{aligned}$$

由 Siegel-Walfisz 定理 (第三章, § 22, (85)), 我们得到

$$\sum_{p \leqslant N} \mathrm{e}^{2\pi \mathrm{i} a p} = \frac{1}{\varphi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} \mathrm{e}^{2\pi \mathrm{i}\frac{ar}{q}} \left(\sum_{n \leqslant N-1} \mathrm{li}\ n(\mathrm{e}^{2\pi \mathrm{i}\beta n} - \mathrm{e}^{2\pi \mathrm{i}\beta(n+1)}) + \mathrm{li}\ N \cdot \mathrm{e}^{2\pi \mathrm{i}\beta N} \right)$$

$$+O(NL^{-4h})$$
$$=\frac{\mu(q)}{\varphi(q)}\left(\sum_{2<n\leqslant N}\mathrm{e}^{2\pi\mathrm{i}\beta n}\int_{n-1}^{n}\frac{\mathrm{d}t}{\log t}\right)+O(NL^{-4h})$$
$$=\frac{\mu(q)}{\varphi(q)}\int_{2}^{N}\frac{\mathrm{e}^{2\pi\mathrm{i}\beta t}}{\log t}\mathrm{d}t+O(NL^{-4h}),$$

最后一步是因为

$$\mathrm{e}^{2\pi\mathrm{i}\beta n}-\mathrm{e}^{2\pi\mathrm{i}\beta t}=2\pi i\beta\int_{t}^{n}\mathrm{e}^{2\pi\mathrm{i}\beta u}\mathrm{d}u\ll\beta(n-t)\ll\frac{n-t}{\tau}.$$

在 E 上, 由第二章 § 15 可有

$$|S(a)|\ll NL^{5-\frac{1}{2}h}.$$

所以得到

$$r(N)=\sum_{\mathfrak{M}}\int_{\mathfrak{M}_{a,q}}(S(a))^{3}\mathrm{e}^{-2\pi\mathrm{i}Na}\mathrm{d}a+O(N^{2}L^{-4})$$
$$=\frac{N^{2}}{2L^{3}}\mathfrak{S}(N)+O(N^{2}L^{-4}\log L),\tag{110}$$

式中

$$\mathfrak{S}(N)=\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^{3}}\right)\prod_{p\mid N}\left(1-\frac{1}{(p-1)^{2}}\right).$$

因为

$$\mathfrak{S}(N)>\prod_{p\mid N}\left(1-\frac{1}{(p-1)^{2}}\right)>\prod_{p}\left(1-\frac{1}{p^{2}}\right)=\frac{6}{\pi^{2}},$$

故得定理.

附注 1　除了 Hardy 与 Littlewood 的开创性工作外, 我们还要提到 Estermann [204),205)] 的两个结果, 这两个结果是在Виноградов 的重大贡献之前得到的. 他证明了: a)[204)] 每一个大的奇整数都能表成形如 $p_1+p_2+p_3p_4$ 的和数, 这里的 p_1, p_2, p_3, p_4 都是素数; b)[205)] 每一个大的整数都是两个素数与一平方数的和.

附注 2　在Виноградов 的工作之后, Линник[12),205)] 与Чудаков[207)] 给出了另外两个证明, 这两证明都以 L- 函数在临界带状区域中的零点分布为基础. 更确切地说, 所用到的性质是 Dirichlet L- 函数 $L(s,\chi)$ 在矩形 $\beta\leqslant\sigma\leqslant 1,|t|\leqslant T$ 中的零点个数等于

$$O(q^{2\beta-1}T^{4(1-\beta)(3-2\beta)^{-1}}\log^{10}T+q^{30}),$$

此处 χ 表一mod q 的原特征, 又记号 O 中所含的常数与 q 无关.

5.2 Виноградов 定理的推广

1) 不少数学工作者研究了有“比例条件”的Гольдбах 问题, 此即

$$N = p_1 + p_2 + p_3, \quad p_i \sim \frac{1}{3}N$$

在 $N \to \infty$ 时成立. 最好的结果是 Haselgrove[203] 所宣布的: 每一个大的奇整数都能表示成

$$N = p_1 + p_2 + p_3, \quad p_i = \frac{1}{3}N + O(N^{\vartheta})$$

的形状, 此处 $\frac{63}{64} < \vartheta < 1$.

2) 另外一些数学工作者 [209][210][211][212] 研究了如下类型的问题: 对于 $s \geqslant 3$, 找出

$$N = a_1p_1 + a_2p_2 + \cdots + a_sp_s$$

的可解条件, 这里的 $a_1, \cdots, a_s$ 都是给定的整数, 而

$$p_\nu \equiv l_\nu (\bmod q), \quad 1 \leqslant \nu \leqslant s.$$

对于 $s \geqslant 3$, 外理这些问题并无本质的困难. 吴方 [213] 更进一步推广了这个问题, 他在某些条件下建立了

$$\sum_{\nu=1}^{m} a_{\mu\nu}p_\nu = b_\mu, \quad \mu = 1, 2, \cdots, n, \ m \geqslant 2n+1, \ 2 \leqslant p_\nu \leqslant P, \ \nu = 1, 2, \cdots, m$$

的解数的渐近公式.

5.3 关于偶数的 Гольдбах 问题的结果

在 Виноградов 的重要工作之后, 很多数学工作者 [214–218] 彼此独立地证明了下面的定理: 几乎全体偶整数都能表成两个素数之和. 华罗庚的结果较旁人的结果稍强, 他证明了 $p_1 + p_2^k$ 表出几乎全体偶数.

Линник 作出了主要的推进.

1)[219] 在 Riemann 猜测真确的假定下, 对于任何 $\varepsilon > 0$ 及对每一大的整数 N, 总可以找到两个素数 p_1 及 p_2, 使

$$|N - p_1 - p_2| < (\log N)^{3+\varepsilon}$$

成立. 又在一较弱的假定下, 也即如果

$$N(\sigma, T) = O(T^{2(1-\sigma)}\log^2 T),$$

则得

$$|N - p_1 - p_2| < (\log N)^7.$$

由 Ingham 关于相继素数的定理, 我们立刻得到 $|N - p_1 - p_2| < N^{\frac{25}{64}+\varepsilon}$. Линник证明, 由此甚至能够得出

$$|N - p_1 - p_2| < N^{0.13}.$$

2)[220] 对于任何给定的正整数 $g > 1$, 恒存在正整数 k_0, 使对任何给定的 $k > k_0$, 每一个 $\equiv kg \pmod 2$ 的大整数都能用

$$p_1 + p_2 + g^{x_1} + \cdots + g^{x_k}$$

表出, 这里的 p_1 与 p_2 都是素数, 而 $x_1, \cdots, x_k$ 都是正整数.

Rényi[19] 做出了另一个有趣的推进.

3) 存在常数 k, 使每一大偶数都是某一素数与另一个不超过 k 个素数的乘积的和. 在此以前, Бухштаб[221] 证明了: 对于任何给定的 $\lambda > 0$, 每一大偶数 N 都能表成 $N = p + N'$ 的形状, 这里的 p 是素数, 而 N' 的素因子都小于 $(\log N)^\lambda$. 这种表法的个数小于 $cN/(\log N \log\log N)$, 而 $c > 0$.

此处, A. Page[157] 证明: 将偶数 N 分解成一个素数与一无平方因子数的方法数等于

$$\prod_p (1 - (p^2 - p)^{-1}) \prod_{p|N} \frac{p^2 - p}{p^2 - p - 1} \int_2^N \frac{\mathrm{d}u}{\log u} + O\Big(\frac{N}{\log^5 N}(\log\log N)^8 \log\log\log N\Big).$$

王元[56] 证明了

4) 在广义 Riemann 猜想正确的假定下, 每一大偶数都是一个素数与一个至多是四个素数乘积的数之和.

Rényi 的证明主要基于Линник[18] 的所谓“大筛法”的某一改进的应用, 就许多关系来说, 这个大筛法与 Brun[14] 的方法相似. 这两个方法的主要不同点是: 在 Brun 的方法中, 由 mod p 的全体剩余类中所除去的类数 k 对一切 p 都是固定的, 但在Линник的方法中, 它们能够随 p 而变. 因为Линник 的大筛法曾为很多数学工作者 [19][114] 成功地应用过, 所以我们现在把它的轮廓作如下的描述: 设 $p_1, \cdots, p_y$ 为任意 y 个适合 $p_i \leqslant \sqrt{N} (i = 1, \cdots, y)$ 的素数.

定理 用 $f(p)$ 表一正值函数, $f(p) < p$, 又命

$$\tau = \min_{i=1,2,\cdots,y} \frac{f(p_i)}{p_i}.$$

假如从序列 1, 2, $\cdots$, N 中除去那些属于 mod $p_i(i=1, \cdots, Y)$ 的 $f(p_i)$ 个确定的剩余类中某一类的整数, 则余下的整数个数不超过

$$\frac{20\pi N}{\tau^2 y}.$$

证　设 $n_1<n_2<\cdots<n_Z\leqslant N$ 为从序列 1, 2, $\cdots$, N 中除去属于 $f(p_i)$ 个 mod $p_i(i=1, 2, \cdots, y)$ 的剩余类中某一类的那些整数后所余下的整数. 命

$$S(\alpha)=\sum_{j=1}^{z}\mathrm{e}^{2\pi\mathrm{i}\alpha n_j},$$

则对 $\delta=\dfrac{\tau}{20\pi N}$, 显然有

$$Z=I=\int_0^1|S(\alpha)|^2\mathrm{d}\alpha\geqslant\sum_{p_j}\sum_{y=1}^{p_j-1}\int_{-\delta}^{+\delta}\left|S\left(\frac{y}{p_j}+x\right)\right|^2\mathrm{d}x=\sum_{p_j}I'_{p_j},$$

这是因为任何两个积分区间都不交迭的原故. 另一方面, 我们有

$$I'_p=\sum_{y=0}^{p-1}\int_{-\delta}^{\delta}\left|S\left(\frac{y}{p}+x\right)\right|^2\mathrm{d}x-\int_{-\delta}^{\delta}|S(x)|^2\mathrm{d}x\geqslant 2\delta p\left(1-\frac{\tau}{10}\right)\sum_{n_i\equiv n_j}\sum_{(\mathrm{mod}\ p)}1-2\delta Z^2.$$

用 a_i 表 $n_1, \cdots, n_Z$ 诸数中与同一 ξ_i 模 p 同余者之个数, 则由 Schwarz 不等式, 可以得出

$$\sum_{n_i\equiv n_j}\sum_{(\mathrm{mod}\ p)}1=\left(\sum_i a_i^2\right)\geqslant\frac{\left(\sum_i a_i\right)^2}{p-f(p)}=\frac{Z^2}{p-f(p)}\geqslant\frac{Z^2}{p}(1+\tau).$$

于是得到

$$Z\geqslant y\delta\tau Z^2=y\frac{\tau^2}{20\pi N}Z^2.$$

证明完毕.

这个定理具有下述的等价形式:

设 $n_1<n_2<\cdots<n_Z\leqslant N$ 为 Z 个正整数. 用 $f(p)$ 表一适合 $f(p)<p$ 的正值函数, 而命

$$\tau=\min_{p\leqslant\sqrt{N}}\frac{f(p)}{p}>0,$$

则至多除了

$$\frac{20\pi N}{\tau^2 Z}$$

个例外的素数外, 对于每一素数 $p\leqslant\sqrt{N}$, 整数 $n_1, \cdots, n_Z$ 一定分落在不少于 $p-f(p)$ 个不同的模 p 剩余类中.

5.4　Waring-Гольдбах 问题

§5.4 与 §5.5 的结果都可在华罗庚的专著 [222] 中找到.

1) 设 $I_s(N)$ 是以素数 $p_1, \cdots, p_s$ 为变量的方程

$$p_1^k + \cdots + p_s^k = N$$

的解数, 于是对于

$$s \geqslant \begin{cases} 2^k + 1, & \text{当} 1 \leqslant k \leqslant 10, \\ 2k^2(2\log k + \log\log k + 2.5), & \text{当} k > 10, \end{cases}$$

可有

$$I_s(N) = \mathfrak{S}(N)\frac{\Gamma^s\left(\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)}\frac{N^{\frac{s}{k}-1}}{(\log N)^s} + O\left(\frac{N^{\frac{s}{k}-1}}{(\log N)^{s+1}}\log\log N\right),$$

此处

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} B_s(N, q),$$

$$B_s(N, q) = \sum_{\substack{h=1\\(h,q)=1}}^{q} (W_{h,q}/\varphi(q))^s \mathrm{e}^{-2\pi\mathrm{i}hN/q},$$

$$W_{h,q} = \sum_{\substack{l=1\\(l,q)=1}}^{q} \mathrm{e}^{2\pi\mathrm{i}hl^k/q}.$$

这里所用的原则是找一 t, 使

$$\int_0^1 \left|\sum_{x=1}^{P} \mathrm{e}^{2\pi\mathrm{i}\alpha x^k}\right|^{2t} \mathrm{d}\alpha \ll P^{2t-k}$$

成立. 由此并按第二章 § 15 的定理 2, 我们得到: 对于 $s > 2t$,

$$\begin{aligned}\int_E \left(\sum_{p\leqslant P} \mathrm{e}^{2\pi\mathrm{i}\alpha p^k}\right)^s \mathrm{e}^{-2\pi\mathrm{i}N\alpha}\mathrm{d}\alpha &\ll (PL^{-\sigma_0})^{s-2t}\int_0^1 \left|\sum_{p\leqslant P} \mathrm{e}^{2\pi\mathrm{i}\alpha p^k}\right|^{2t}\mathrm{d}\alpha \\ &\ll P^{s-2t}L^{-s_1}\int_0^1 \left|\sum_{x=1}^{P} \mathrm{e}^{2\pi\mathrm{i}x^k\alpha}\right|^{2t}\mathrm{d}\alpha \ll P^{s-k}L^{-s_1},\end{aligned}$$

这里的 E 就是所谓“劣弧”.

这个结果能够推广到

$$f_1(p_1)+\cdots+f_s(p_s).=N$$

的问题, 此处 $f_1,\ \cdots,\ f_s$ 为 s 个首项系数为正的整值多项式.

2) 设 $p^{\Theta}||k$, 而

$$K=\prod_{(p-1)|k} p^{\gamma},$$

这里的 γ 当 $p=2$ 而 $2|k$ 时等于 $\Theta+2$, 在其他情形, 则等于 $\Theta+1$.

用 $H(k)$ 表示具有下述性质的最小整数 s: 它使每一充分大的 $\equiv s(\text{mod } K)$ 的整数都能表成 s 个素数的 k 次乘幂之和. 通过研究算术性状, 我们便由 1) 得出

$$H(k)\leqslant\begin{cases}2^k+1, & \text{当}1\leqslant k\leqslant 10,\\ 2k^2(2\log k+\log\log k+2.5), & \text{当}k>10.\end{cases}$$

因此, 每一大奇数都是三个素数的和; 每一个 $\equiv 5(\text{mod } 24)$ 的大整数都是五个素数的平方之和; 每一大奇数都是九个素数的立方之和.

更进一步, 我们有

$$H(k)\leqslant 2k+2m+7,$$

此处

$$m=\left[\frac{\log\dfrac{1}{2}b+\log\left(1-\dfrac{2}{k}\right)}{-\log\left(1-\dfrac{1}{k}\right)}\right],\quad b=\begin{cases}2k^2(2\log k+\log\log k+3), & \text{当}k>12,\\ 2^{k-1}, & \text{当}k\leqslant 12,\end{cases}$$

读者注意, $2k+2m+7\sim 4k\log k$.

借助于 Davenport 的引理, 我们还能得到

$$H(4)\leqslant 15,\ H(5)\leqslant 25,\ H(6)\leqslant 37,\ H(7)\leqslant 55,\ H(8)\leqslant 75.$$

5.5　问题的变形

Halberstam[223] 证明: 几乎全体正整数 m 都能表成 $p_1^2+p_2^3+x^3$ 的形状, 这里的 p_1,p_2 都是素数, 而 x 为一正整数.

Prachar[224] 证明: 几乎全体偶整数都能表成

$$p_1^2+p_2^3+p_3^4+p_4^5$$

的形状, 这里的 p_1, p_2 p_3 p_4 都是素数; 他还证明了, 全体充分大的奇数都能表成

$$p_1+p_2^2+p_3^3+p_4^4+p_5^5$$

的形状.

设 $c>1$ 非整数, И. И. Шапиро-Пятецкий[225] 证明: 对于任何给定的 $\varepsilon>0$, 存在 $N_0=N_0(\varepsilon)$, 使对任何实数 $N>N_0$, 当 $r\geqslant H(c)$ 时, 不等式

$$|p_1^c+\cdots+p_r^c-N|<\varepsilon$$

都有素数解. 他还证明了

$$\overline{\lim_{c\to\infty}}\frac{H(c)}{c\log c}\leqslant 4.$$

5.6 齐次问题 (请参考 Марджанишвили[226])

1) 对于任何整数 $k\geqslant 2$, 用 $I(N_1,\ \cdots,\ N_k)$ 表示满足方程组

$$\begin{aligned}&p_1^k+\cdots+p_s^k=N_k,\\&\cdots\cdots\\&p_1+\cdots+p_s=N_1\end{aligned}$$

的素数组 $p_1,\ \cdots,\ p_s$ 的组数.

设 s_0 为由下表给出的数值:

k	2	3	4	5	6	7	8	9	10	$\geqslant 11$
s_0	7	19	49	113	243	417	675	1083	1773	$2k^2(3\log k+\log\log k+4)$

并置 $[N_k^{\frac{1}{k}}]=P$, 则对 $s\geqslant s_0$, 渐近公式

$$I(N_k,\ \cdots,\ N_1)=b_1P^{s-\frac{1}{2}k(k+1)}L^{-s}\mathfrak{S}(N_k,\ \cdots,\ N_1)+O(P^{s-\frac{1}{2}k(k+1)}L^{-s-1}\log L)$$

成立, 此处

$$b_1=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\left(\int_0^1 \mathrm{e}^{2\pi\mathrm{i}(\gamma_k x^k+\cdots+\gamma_1 x)}\mathrm{d}x\right)^s \mathrm{e}^{-2\pi\mathrm{i}(N_kP^{-k}\gamma_k+\cdots+N_1P^{-1}\gamma_1)}\mathrm{d}\gamma_k\cdots\mathrm{d}\gamma_1,$$

$$\mathfrak{S}(N_k,\ \cdots,\ N_1)=\sum_{q_1,\cdots,q_k=1}^{\infty}A(q_k,\ \cdots,\ q_1),$$

$$A(q_k,\ \cdots,\ q_1)=\sum_{h_1,\cdots,h_k}{}' T^s\mathrm{e}^{-2\pi\mathrm{i}(\frac{h_kN_k}{q_k}+\cdots+\frac{h_1N_1}{q_1})},$$

$$T = \frac{1}{\varphi(Q)} \sum_{x}{}' \mathrm{e}^{2\pi \mathrm{i}\left(h_k \frac{x^k}{q_k} + \cdots + h_1 \frac{x}{q_1}\right)},$$

Q 是 $q_1, \cdots, q_k$ 的最小公倍数, $h_1 \cdots, h_k$ 分别通过 $\bmod q_1, \cdots, \bmod q_k$ 的缩剩余系, 而 x 则通过 $\bmod Q$ 的缩剩余系.

2) 我们也得到了保证主项确实大于误差项的两个条件, 它们是 1)"阶条件"与 2)"同余条件". 实际上, 1) 保证了方程组:

$$x_1^h + \cdots + x_s^h = N_h, \quad 1 \leqslant h \leqslant k$$

具有正解，而 2）保证了同余组:

$$x_1^h + \cdots + x_s^h \equiv N_h, \quad (\bmod q), \quad 1 \leqslant h \leqslant k$$

对于全体 $q \geqslant 1$ 都可解.

更多的结果可在 §5.4 开始时所引到的华罗庚的专著 23) 中找到.

第6章　一致分布

6.1　定义与 Weyl 判别法则

设 $f(x)$ 为一实函数. 对于给定的满足 $0 \leqslant a \leqslant b \leqslant 1$ 的 a 与 b, 用 $N(P; a, b)$ 表示使

$$a \leqslant \{f(n)\} < b \tag{111}$$

成立的整数 $n \leqslant P$ 的个数, 这里的 $\{f(n)\}$ 表示 $f(n)$ 的分数部分. 如果

$$\lim_{P\to\infty} \frac{N(P; a, b)}{P} = b - a, \tag{112}$$

则称 $f(x)$ 模 1 一致分布.

Weyl[20] 给出了下面的重要判别法则.

定理 1　如果 $f(x)$ 模 1 一致分布, 则对任何黎曼可积函数 $w(t)$, 都有

$$\lim_{P\to\infty} \frac{1}{P} \sum_{x=1}^{P} w(\{f(x)\}) = \int_0^1 w(t)\mathrm{d}t. \tag{113}$$

这几乎可以从黎曼积分的定义立刻导出. 又取 $w(t) = 1$(当 $a \leqslant x < b$ 时), $w(t) = 0$(在其他点上), 就立刻得到逆定理.

在黎曼可积函数的集合中, 我们选出一个特殊序列

$$\mathrm{e}^{2\pi\mathrm{i}ht}, \quad h = 0, \pm 1, \pm 2, \cdots. \tag{114}$$

(114) 的线性包给出每一黎曼可积函数, 这就建议了

定理 2(Weyl 判别法则)　当且仅当

$$\lim_{P\to\infty} \frac{1}{P} \sum_{x=1}^{P} \mathrm{e}^{2\pi\mathrm{i}hf(x)} = 0$$

对于任何确定的整数 $h \neq 0$ 都成立时, 函数 $f(x)$ 模 1 一致分布.

证　充分性的证明. 设 $G(t)$ 为一具有周期 1 的函数, 当 $0 \leqslant t < \gamma$ 时, $G(t) = 1$; 当 $\gamma \leqslant t < 1$ 时, $G(t) = 0$. 于是

$$N(P; 0, \gamma) = \sum_{x=1}^{P} G(f(x)).$$

命 η 为一适合不等式 $2\eta < \gamma$ 与 $2\eta < 1-\gamma$ 的正数. 我们作出两个辅助函数 $G_1(t)$ 与 $G_2(t)$, 它们都有周期 1, 并且适合

$$G_2(t) \leqslant G(t) < G_1(t).$$

又 $G_1(t) = 1$(当 $0 \leqslant t \leqslant \gamma$), $= 0$(当 $\gamma+\eta \leqslant t \leqslant 1-\eta$), 而在 $-\eta \leqslant t \leqslant 0$ 与 $\gamma \leqslant t \leqslant \gamma+\eta$ 中它为线性函数; $G_2(t) = 1$(当 $\eta \leqslant t \leqslant \gamma-\eta$), $= 0$(当 $\gamma \leqslant t \leqslant 1$), 在 $0 \leqslant t \leqslant \eta$ 与 $\gamma-\eta \leqslant t \leqslant \gamma$ 中也为线性函数. 因为 G_1, G_2 都为连续, 故有一致收敛的傅里叶级数展开:

$$G_1(t) = \gamma + \eta + \sum_{h=1}^{\infty}(a_h \mathrm{e}^{2\pi i h t} + b_h \mathrm{e}^{-2\pi i h t}),$$
$$G_2(t) = \gamma - \eta + \sum_{h=1}^{\infty}(a'_h \mathrm{e}^{2\pi i h t} + b'_h \mathrm{e}^{-2\pi i h t}).$$

在这两级数中, 都置 $t = f(x)$, 并对 $x = 1, 2, \cdots, P$ 相加, 就得到

$$\lim_{P\to\infty} \frac{N(P;0,\gamma)}{P} = \gamma.$$

我们先研究线性的情形. 因为对于任何整数 $h \neq 0$ 与对任何无理数 α, 都有

$$\lim_{P\to\infty} \frac{1}{P}\left|\sum_{x=1}^{P} \mathrm{e}^{2\pi i h \alpha x}\right| \leqslant \lim_{P\to\infty} \min(1, \frac{1}{|\sin \pi h\alpha|P}) = 0.$$

故得

定理 3　对于任何实无理数 α, 序列

$$\alpha, 2\alpha, 3\alpha, \cdots$$

模 1 一致分布.

由定理 2 我们能够导出

定理 4　设 $f(x)$ 为一非常数的并且至少有一无理系数的多项式, 则序列

$$f(x), \quad x = 1, 2, \cdots$$

模 1 一致分布.

Van der Corput[227] 将此概念加以推广, 从而得到了

定理 5　如果对于任何固定的正整数 q, $f(x+q) - f(x)$ 模 1 一致分布, 则函数 $f(x)$ 模 1 一致分布.

Weyl 也证明了

定理 6　设 $g(x)(x=1,2,3,\cdots)$ 为一列互不相同的整数, 则对几乎全体 α, 函数 $ag(x)$ 模 1 一致分布 (这里的 "几乎全体" 是按勒具格意义而言).

为了证明这个定理, 我们利用恒等式

$$\int_0^1\left|\frac{1}{N}\sum_{x=1}^{N}\mathrm{e}^{2\pi\mathrm{i}hag(x)}\right|^2\mathrm{d}\alpha=\frac{1}{N},\quad \alpha\neq 0,\ h\text{是非0整数}.$$

由此我们能够估计那些使被积函数大于一个给定正数的 α 所成集合测度的上界.

另一方面, 对于任何给定的实数 α, 我们能够容易地构造出一列整数 $g(x)(x=1,2,\cdots)$, 使 $\alpha g(x)(x=1,2,\cdots)$ 模 1 并不一致分布.

Koksma[228] 用 Weyl 的方法证明了

定理 7　对于几乎全体实数 $\alpha\geqslant 1$, 序列 $\alpha^x(x=1,2,\cdots)$ 都模 1 一致分布.

但到现在为止, 人们还不知道 e^x 是否模 1 一致分布.

6.2　误差项的估计

采用 §36 中的记号, 我们称函数

$$R(P)=N(P;a,b)-(b-a)P \tag{115}$$

为误差项, 而称

$$D(P)=R(P)/P \tag{116}$$

为离差. 如果 $f(x)$ 模 1 一致分布, 则

$$R(P)=o(P). \tag{117}$$

根据第二章 §7 的结果, 我们有下面的

定理 1(Виноградов[229])　设 $k\geqslant 2, P\geqslant 1$, 又设

$$f(x)=ax^k+a_1x^{k-1}+\cdots+a_k,$$

$$\left|a-\frac{h}{q}\right|<\frac{1}{q^2},\quad (h,q)=1,\ 1\leqslant q\leqslant P^k,$$

则对 $f(x)$ 的离差 $D(P)$, 我们得到: 对于任何 $\varepsilon>0$,

$$D(P)=O(L),\quad L=P^{\varepsilon}(P^{-1}+q^{-1}+qP^{-k})^{2^{1-k}}$$

成立.

为了证明这个定理, 取 $\eta=P^{-2^{1-k}}<\dfrac{1}{3}$ 及

$$0<\gamma<1-2\eta,$$

并如 §6.1 中那样定义 $G_1(t)$ 与 $G_2(t)$, 于是不难得到

$$|a_h|\leqslant\min\left(\frac{1}{h},\frac{1}{\eta h^2}\right),\quad |b_h|\leqslant\min\left(\frac{1}{h},\frac{1}{\eta h^2}\right).$$

由此

$$\begin{aligned}N(P;0,\gamma)&=\sum_{x=1}^{P}G(f(x))\leqslant\sum_{x=1}^{P}G_1(f(x))\\&=(\gamma+\eta)P+2\sum_{h=1}^{P}\frac{1}{h}\left|\sum_{x=1}^{P}e^{2\pi ihf(x)}\right|+O(P^{1-2^{1-k}}).\end{aligned}$$

证明的主要部分在于二重指数和的估计, 而由第二章 §7 知道它 $\ll PL$, 因此

$$N(P;0,\gamma)\leqslant\gamma P+O(PL).$$

类似地, 我们用 $G_2(x)$ 代替 $G_1(x)$, 便得

$$N(P;0,\gamma)\geqslant\gamma P+O(PL).$$

所以

$$R(P)=O(PL).$$

如用Виноградов更精密的结果, 我们能够得出

定理 2　设 $k\geqslant 11$,

$$f(x)=a_{k+1}x^{k+1}+\cdots+a_1x$$

为一实系数多项式; 又设 s 为 $k+1,\cdots,2$ 诸数之一, 并且

$$\left|a_s-\frac{h}{q}\right|<\frac{1}{q^2},\quad (h,q)=1,\ q>0,$$

则有

$$R(P)=O(P^{1-\rho}),$$

此处

$$\rho=\tau/3k^2\log\frac{12k(k+1)}{\tau},$$

τ 随 P 与 q 而变, 它的定义如下:

$$q = c_1 P^{\tau}, \quad 当 1 < q \leqslant c_1 P,$$
$$\tau = 1, \quad 当 c_1 P \leqslant q \leqslant c_2 P^{s-1},$$
$$q = c_2 P^{s-\tau}, \quad 当 c_2 P^{s-1} \leqslant q \leqslant c_3 P^s,$$

c_1, c_2, c_3 都是确定的正常数.

对于 $2 \leqslant k \leqslant 10$, 用 Weyl 的估计 (第二章 §7), 我们得到一个类似的结果. 对于线性与二次多项式 $f(x)$, 大量的更进一步的结果已为很多数学工作者所获得 (参见 Koksma[230]).

更一般地, Erdös 与 Turán[231] 证明了: 如果 $\varphi_1, \cdots, \varphi_P$ 都是实的, 又若对全体正整数

$$k \leqslant m = m(P),$$

不等式

$$\left|\sum_{\nu=1}^{P} \mathrm{e}^{2\pi \mathrm{i} k \varphi_\nu}\right| \leqslant \psi(k)$$

成立, 则

$$R(P) = O\left(\frac{P}{m+1} + \sum_{k=1}^{m} \frac{\psi(k)}{k}\right).$$

它是 Koksma[230] 一个定理的改进.

附注 如果 $\{f(1)\}, \{f(2)\}, \cdots$ 构成一无穷序列, 则有

$$\varlimsup_{P \to \infty} \overline{R}(P) \frac{\log \log \log P}{\log \log P} \geqslant \frac{1}{2},$$

此处

$$\overline{R}(P) = \varlimsup_{0 \leqslant a < b \leqslant 1} |N(P; a, b) - (b-a)P|.$$

因此, 不可能有实函数 $f(x)$, 使它对 $x = 1, 2, \cdots$ 有无穷多个不相同的分数部分, 且有有界的误差项. 这个结果属于 van Aardenne-Ehrenfest[232], 它回答了 van der Corput 提出的一个问题.

6.3 以素数为变数的函数的分布

一旦Виноградов证明了他的著名的 “三素数” 定理, 他的方法实际上也包含了关于函数 αp 的模 1 一致分布问题的解决, 这里的 p 跑过全体素数. 事实上, 由 Weyl 判别法则可知, 充分而又必要的是去证明: 对于任何固定的整数 $h \neq 0$,

$$\sum_{p \leqslant P} \mathrm{e}^{2\pi \mathrm{i} \alpha h p} = O(\pi(P)), \quad \alpha 是一无理数. \tag{118}$$

命 $\tau = P(\log P)^{-\sigma}(\sigma \geqslant 16)$, 又命 $\frac{p_n}{q_n}$ 为 αh 的第 n 个渐近分数; 对于任何给定的 $\varepsilon > 0$, 取 q_{n_0} 很大, 使对任何整数 $q > \frac{q_{n_0}}{2}$, 恒有

$$\varphi(q) > \frac{1}{\varepsilon}.$$

又取 P_0 很大, 使 $\tau_0 = P_0(\log P_0)^{-\sigma} > q_{n_0}$, 则对任何 $P > P_0$, 恒存在一 $n \geqslant n_0$, 使不等式

$$q_n \leqslant \tau < q_{n+1}$$

成立. 于是

$$\left|h\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n \tau}.$$

如果 $q_n \leqslant \log^\sigma P$, 则由 Siegel-Walfisz 定理 (第三章, §22, (85)), 我们得到

$$\sum_{p \leqslant P} \mathrm{e}^{2\pi \mathrm{i} h\alpha p} = \frac{\mu(q_n)}{\varphi(q_n)} \int_2^P \frac{\mathrm{e}^{2\pi \mathrm{i}(h\alpha - \frac{p_n}{q_n})t}}{\log t} \mathrm{d}t + O(P\mathrm{e}^{-c\sqrt{\log P}}).$$

由此导出 (118). 如果 $\log^\sigma P < q_n < P(\log P)^{-\sigma}$, 则用Виноградов定理 (第二章, §15),

$$\sum_{p \leqslant P} \mathrm{e}^{2\pi \mathrm{i} h\alpha p} = O(P(\log P)^{-3}),$$

也得到 (118).

Виноградов对大多数有兴趣的情形获得了更好的误差项. 他用到下面的估计:

定理 1　假设 τ 满足不等式

$$P^{\frac{1}{2}} \leqslant \tau \leqslant P\mathrm{e}^{-(\log P)^{\varepsilon_0}},$$

又设

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{1}{q\tau}, \quad (h, q) = 1$$

及 $\mathrm{e}^{(\log P)^{\varepsilon_0}} \leqslant q \leqslant \tau$, 并命 $\Delta = (q^{-1} + qP^{-1})^{\frac{1}{2}}$,

$$S = \sum_{m=1}^{K} \left|\sum_{p \leqslant P} \mathrm{e}^{2\pi \mathrm{i} mp\alpha}\right|,$$

而 $K \ll \Delta^{-2}$, 则有

$$S \ll KP(\Delta^{1-\varepsilon} + P^{-\frac{1}{5}+\varepsilon}).$$

用此定理及 §6.2 的方法, 我们得到

定理 2　在与定理 1 相同的假定下, 用 $H(P)$ 表示适合

$$\{\alpha p\} \leqslant \beta, \quad p \leqslant P$$

的素数 p 的个数, 此处 $0 < \beta < 1$, 则有

$$H(P) = \beta\pi(P) + O(P\gamma),$$

而

$$\gamma = (q^{-1} + qP^{-1})^{\frac{1}{2}-\varepsilon} + p^{-\frac{1}{5}+\varepsilon}.$$

特别, 如果 α 为一具有有界部分商的无理数, 则能这样选取 q, 使它落在 $\sqrt{P}$ 的两个常数倍的中间. 于是得到

$$H(P) = \beta\pi(P) + O(P^{\frac{4}{5}+\varepsilon}),$$

这里的误差项异常地好. 与作为 P 的函数的 $\pi(P)$ 相比, 它比后者的渐近表示中任何已得的误差项要优越得多.

设 $f(x)$ 为一多项式, 它的首项系数是无理数, 则 $\{f(p)\}$ 模 1 一致分布 [233]. 对于无理数 $\alpha, \{\alpha p\}$ 为模 1 一致分布的结果, 先是由 Turán[234] 在广义 Riemann 假设下证得的.

6.4　$\{a^x\}$ 的分布

在 §6.1 中, 我们已经看到, 对于几乎全体实数 $a, \{a^x\}$ 都是一致分布的. 但对某一给定的 $a, \{a^x\}$ 是否一致分布的问题, 至今还未获得解决. 特别, 我们还不知道 $\{e^x\}$ 是否一致分布.

Постников[235]用Виноградов方法证明了下面的判别法则.

定理 1　设 q 为一 $\geqslant 2$ 的整数, α 为一实数, 用 $N(P;a,b)$ 表示使 $a \leqslant \{\alpha q^x\} \leqslant b(0 \leqslant a < b \leqslant 1)$ 的整数 $x \leqslant P$ 的个数. 如果存在常数 $c > 1$ 及 $k > 0$, 使

$$\overline{\lim_{P\to\infty}} \frac{N(P;a,b)}{P} \leqslant c(b-a)\left(1 + \log\frac{1}{b-a}\right)^k$$

对任何 a 与 b 都成立, 则函数 αq^x 模 1 一致分布.

Коробов[236]得到了下面的结果.

定理 2　设 $q \geqslant 2$ 为一固定的整数,

$$\rho_n(q) = \delta_1 \cdots \delta_{q^n+n-1}, \quad 0 \leqslant \delta_i \leqslant q-1, \quad 1 \leqslant i \leqslant q^n + n - 1,$$

此处 $\delta_1\delta_2\cdots\delta_n, \delta_2\delta_3\cdots\delta_{n+1}, \cdots, \delta_{q^n}\delta_{q^n+1}\cdots\delta_{q^n+n-1}$ 等 q^n 个数互不相同; 又命

$$\rho_n'(q) = \delta_1\cdots\delta_{q^n},$$

而 $\psi(\mu)$ 为适合 $\lim\limits_{\mu\to\infty}\psi(\mu)=\infty$ 的任何正整值函数; 最后, 命

$$\alpha = 0\cdot\underbrace{\rho_1'(q)\cdots\rho_1'(q)}_{\psi(1)}\underbrace{\rho_2'(q)\cdots\rho_2'(q)}_{\psi(2)}\cdots\underbrace{\rho_\mu'(q)\cdots\rho_\mu'(q)}_{\psi(\mu)}\cdots,$$

则 $\{\alpha q^x\}$ 一致分布.

定理 3　设 $\varphi(x)$ 为一实值函数, 对于任意给定的不全为零的整数 $m_1,\cdots,m_s$, 假设和数

$$m_1\varphi(x+1)+\cdots+m_s\varphi(x+s),\quad x=1,2,\cdots$$

模 1 一致分布, 又命

$$\beta=\sum_{k=1}^{\infty}[\{\varphi(k)\}q]/q^k,$$

则 $\{\beta q^x\}$ 一致分布.

Коробов[237]还证明了: 如果 $\lambda>1$ 为一代数整数, 并且适合某种条件, 则 $\{\alpha\lambda^x\}$ 一致分布, 此处

$$\alpha=\sum_{i=1}^{\infty}\frac{\varphi(i)\gamma_i}{p_i(\lambda^{\tau_i}-1)}\left(\frac{1}{\lambda^{n_i}}-\frac{1}{\lambda^{n_{i+1}}}\right),$$

式中的 $p_i, n_i, \tau_i, \varphi(i)$ 都是整数, γ_i 为一有理数, 它们每一个都受到某些条件的限制.

6.5　不定不等式

设 $f(x)$ 模 1 一致分布, 它有离差 $D(P)$, 亦即, 适合

$$\gamma-\varepsilon\leqslant\{f(x)\}\leqslant\gamma+\varepsilon$$

的整数 $x\leqslant P$ 的个数等于 $2\varepsilon P+PD(P)$. 于是对于 $\varepsilon>\frac{1}{2}|D(P)|$, 存在整数 x, 使

$$|\{f(x)\}-\gamma|<\varepsilon \tag{119}$$

成立. 特别, 如设 $k\geqslant 11$ 及

$$f(x)=\alpha_{k+1}x^{k+1}+\cdots+\alpha_1 x,\quad \left|\alpha_s-\frac{h}{q}\right|<\frac{1}{q^2},$$

则由 §6.2 定理 2, 我们得出：存在整数 $x \leqslant P$, 使对大的 P,

$$|\{f(x)\}-\gamma| \ll P^{-\rho}$$

成立. Виноградов推广了这个定理.

定理　设

$$f(x)=\alpha_h x^h+\cdots+\alpha_k x^k$$

为一实系数多项式, 此处 $h<\cdots<k$ 都是正整数. 又设 α_l 为 x^l 的系数, 并且

$$\left|\alpha_l-\frac{a}{q}\right|<\frac{1}{q^2}, \quad (a, q)=1.$$

用 g 表示 $f(x)$ 的非零系数的个数, 而 D 表它们的足标的和, 则必存在一个具有下之性质的 $c_0(k)$：对于 $q>c_0(k)$, 存在整数 x, 使

$$|\{f(x)\}-\gamma|<q^{-\rho}, \quad 0<x<q^{\frac{2}{l}}$$

成立, 此处

$$\rho=\frac{\log D}{4kgl(\log D+1)\log(D\log D+D)}.$$

第 7 章　其他数论函数

7.1　引　　言

如果 $f(n)$ 对正整数 n 有定义, 则称它为一数论函数. 如果对 $(m,m')=1$, 有 $f(m)f(m')=f(mm')$, 则称它为积性的. 又如 $f(m)f(m')=f(mm')$ 常成立, 则称它为完全积性的.

下列数论函数在文献中经常出现.

a) Möbius 函数 $\mu(n)$ 与其绝对值 $|\mu(n)|$ 都是积性的.

b) Euler 函数 $\varphi(n)$, 它表示 $\leqslant n$ 且与 n 互素的正整数个数.

c) 除数函数 $d(n)$, 它表示 n 的正因子个数, 或更一般的有

$$\sigma_a(n)=\sum_{d|n}d^a.$$

d) 函数 $r(n)$, 它表示将整数 n 分解成两个平方之和的方法数, 或更一般的有

$$r_m(n)=\sum_{n_1^2+\cdots+n_m^2=n}1.$$

可以举出大量的数论函数, 但在这里, 我们只准备给出其中极少数几个能与数论的解析方法紧密结合的数论函数的结果.

有关数论函数 $f(n)$ 的问题, 主要是关于 $f(n)$ 的性状与对大的 $n, f(n)$ 的均值性状的问题.

对于前一种情形, 我们讨论下述各种问题: 设法找一函数 $\psi(n)$, 使 $|f(n)|<\psi(n)$ 对全体 n, 对几乎全体 n, 或对无穷多个 n 成立. 对于函数 $\dfrac{1}{f(n)}$, 也有类似的问题, 它也是一数论函数.

例如, 我们有 $\varphi(n)\leqslant n-1$ 及

$$\mathrm{e}^{-\gamma}=\varliminf_{n\to\infty}\frac{\varphi(n)\log\log n}{n}.$$

又有

$$2 \leqslant d(n),$$

$$\varlimsup_{n\to\infty} \frac{\log d(n) \log\log n}{\log n} = \log 2,$$

$$\varlimsup_{n\to\infty} \frac{\sigma(n)}{n \log\log n} = \mathrm{e}^{\gamma},$$

此处 γ 表 Euler 常数.

第二种情形, 也就是关于平均值的问题, 在解析数论中占有更重要的地位. 通常, 我们能够给出一个渐近公式

$$\sum_{n\leqslant N} f(n) = P(N) + R(N),$$

$\dfrac{R(N)}{P(N)}$ 于 $N\to\infty$ 时趋向于 0. 主要问题在于寻求 $R(N)$ 的最优阶. 还有另外一些问题, 如关于 $R(N)$ 的 Ω- 结果与 $R(N)$ 的平均阶的问题等.

对于数论函数 $f(n)$, 我们定义

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \quad s = \sigma + \mathrm{i}t$$

为它的生成函数. 通常, 它在某一右半平面如 $\Re s > \sigma_0$ 中正则. 大家知道

$$\sum_{n\leqslant x} f(n) = \frac{1}{2\pi\mathrm{i}} \int_{\sigma_1 - \mathrm{i}\infty}^{\sigma_1 + \mathrm{i}\infty} F(s) \frac{x^s}{s} \mathrm{d}s, \quad \sigma_1 > \sigma_0.$$

常用的办法是将积分途径移到 $\sigma = -\infty$, 而得到一个与 Riemann-von Mangoldt 素数公式类似的显式, 或者将它移到某一直线 [238], 而得到一个附有误差项的渐近公式.

7.2　$\sum\limits_{n\leqslant x} \sigma_a(n)$ 与 $\sum\limits_{n\leqslant x} r_m(n)$ 的表示式

命

$$F(z) = \sum_{n=1}^{\infty} a_n \lambda_n^{-2z-k},$$

$\{a_n\}$ 与 $\{\lambda_n\}$ 为两个给定的序列. 为了这里的目的, 我们假定 $a_n = O(n^{\varepsilon})$ 及

$$n^{\frac{1}{2}} \ll \lambda_n \ll n^{\frac{1}{2}}.$$

于是从著名的公式

$$\pi \mathrm{i} e^{\frac{1}{2}k\pi \mathrm{i}} H_k^{(1)}(2\mathrm{i}s) = \frac{1}{2\pi \mathrm{i}} \int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} s^{-2z} \Gamma\left(z - \frac{k}{2}\right) \Gamma\left(z + \frac{k}{2}\right) \mathrm{d}z,$$

其中 $H_k^{(1)}(s)$ 为第一类 Hankel 函数, 我们能够得到

$$\begin{aligned} f_k(s) &= \frac{1}{2\pi \mathrm{i}} \int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} s^{-2z} F(z) \Gamma\left(z - \frac{k}{2}\right) \Gamma\left(z + \frac{k}{2}\right) \mathrm{d}z \\ &= \pi \mathrm{i} e^{\frac{1}{2}k\pi \mathrm{i}} \sum_{n=1}^{\infty} a_n \lambda_n^{-k} H_k^{(1)}(2\mathrm{i}\lambda_n s). \end{aligned}$$

另一方面, 如将积分途径移到 $\sigma = -a$, 这里的 a 适合不等式

$$\frac{1}{2}k < a < \min\left(\frac{1}{2}k + 1, 2\left[\frac{1}{2} + \frac{k}{2}\right] + 1 - \frac{k}{2}\right),$$

则得

$$f_k(s) = \varphi_k(s) + \frac{1}{2\pi \mathrm{i}} \int_{-a-\mathrm{i}\infty}^{-a+\mathrm{i}\infty} s^{-2z} F(z) \Gamma\left(z - \frac{k}{2}\right) \Gamma\left(z + \frac{k}{2}\right) \mathrm{d}z,$$

此处 $\varphi_k(s)$ 为求积函数在带状区域 $-a < x < c$ 中的各个留数之和. 故若 $F(z)$ 在直线 $\sigma = -a$ 上的性状为已知, 则由此我们能够导得 $f_k(s)$ 的另一公式. 将这两公式代入积分

$$\frac{1}{2\pi \mathrm{i}} \int_{c-\mathrm{i}\tau'}^{c+\mathrm{i}\tau'} f_k(s) I_{1+k}(4\pi \mathrm{i} s\sqrt{x}) \left(1 - \frac{s^4}{\tau^4}\right)^{\lambda} \mathrm{d}s,$$

而取适当的 λ, τ', τ, 我们便能得到 $\sum\limits_{n \leqslant x} a_n$ 的一个表示式. 当 $a_n = \sigma_a(n)$ 时, 我们取 $F(s) = \zeta\left(s - \frac{a}{2}\right)\left(s + \frac{a}{2}\right), \lambda_n = 4\pi\sqrt{n}$; 而对 $a_n = r_m(n)$, 则取

$$k = \frac{m}{2} - 1, \quad \lambda_n = 2\pi\sqrt{n}, \quad F(s) = \zeta_m\left(s + \frac{k}{2}\right),$$

此处 $\zeta_m(s)$ 为在 $\sigma > \dfrac{m}{2}$ 时由等式

$$\zeta_m(s) = \sum{}' \frac{1}{(n_1^2 + \cdots + n_m^2)^s}.$$

表示的 Epstein ζ- 函数.

Oppenheim[239] 证明了

$$\sum_{n \leqslant x} \sigma_a(n) - \frac{1}{2}\sigma_a(x) = \Phi_a(x) - x^{\frac{1}{2}+\frac{a}{2}} \sum_{n=1}^{\infty} \frac{\sigma_a(n)}{n^{\frac{1}{2}+\frac{a}{2}}} \left\{ \sin\frac{1}{2}a\pi I_{1+a}(4\pi\sqrt{nx}) \right.$$

$$+\cos\frac{1}{2}a\pi\left[Y_{1+a}(4\pi\sqrt{nx})+\frac{2}{\pi}K_{1+a}(4\pi\sqrt{nx})\right]\Big\}, \quad (120)$$

这里的 $\Phi_a(x)$ 为 $z^{-1}\zeta(z)\zeta(z-a)x^z$ 的各个留数之和; 级数在 $|a|\geqslant\frac{1}{2}$ 时对于任何 $\varepsilon>0$ 都 $\left(R,n,|a|-\frac{1}{2}+\varepsilon\right)$ 可和, 而在 $|a|<\frac{1}{2}$ 时收敛. 又

$$\sum_{n\leqslant x}r_m(n)-\frac{1}{2}r_m(x)=\frac{\pi^{\frac{m}{2}}}{\Gamma\left(1+\frac{m}{2}\right)}x^{\frac{m}{2}}+x^{\frac{m}{2}}\sum_{n=1}^{\infty}\frac{r_m(n)}{n^{\frac{1}{4}m}}I_{\frac{1}{2}m}(2\pi\sqrt{nx}),$$

这里的级数在 $m=2$ 时收敛, 而在 $m>2$ 时 $\left(R,n,\frac{1}{2}(m-3)+\varepsilon\right)$ 可和.

在这两种情形中, 可和性与收敛性在任何不包含 x 的整数值的闭区间中都是一致的.

对于具有行列式 D 的任何正定二次型 $Q(x_1,\cdots,x_m)=\sum a_{ij}x_ix_j$, 也有类似的结果. 亦即, 如用 $r_m(n)$ 表示 $Q=n$ 的解数, 则相应地可以得到

$$\sum_{n\leqslant x}r_m(n)-\frac{1}{2}r_m(x)=\frac{\pi^{\frac{m}{2}}x^{\frac{m}{2}}}{\sqrt{D}\Gamma\left(\frac{m}{2}+1\right)}-1+\frac{1}{\sqrt{D}}x^{\frac{m}{4}}\sum_{n=1}^{\infty}\frac{r_m(n)}{n^{\frac{m}{4}}}I_{\frac{1}{2}m}(2\pi\sqrt{nx}).$$

7.3 一般区域中的整点问题

Виноградов与 van der Corput 互相独立地发展了处理一般区域中的整点问题的方法, 他们的方法也包含了 Voronoi 与 Sierpinski 的结果. Виноградов的方法比较早些, 也比较简单些 (就其在 "数论基础"[68] 一书中的最后叙述形式而言), 但由它所得的结果要比用 van der Corput 方法得到的差一对数因子 (这对圆内整点问题与除数问题都不生影响). 另一方面, Jarnik 指出, van der Corput 定理是它这类定理中的最优的. Van der Corput 的结果叙述如下:

设函数 $f(u)$ 在区间 $\frac{1}{2}\leqslant u\leqslant w$ 中具有二阶连续导数, 并且 $f\left(\frac{1}{2}\right)>2, 0<f'(u)<1, f''(u)>z^{-3}, z>1$. 用 $\mathfrak{G}$ 表示区域 $\frac{1}{2}\leqslant u\leqslant w, \frac{1}{2}\leqslant v\leqslant f(u)$. 设 $I(\mathfrak{G})$ 为 $\mathfrak{G}$ 的面积, 而 $A(\mathfrak{G})$ 为 $\mathfrak{G}$ 中所含的整点个数, 则有

$$|A(\mathfrak{G})-I(\mathfrak{G})|\ll z^2. \quad (121)$$

Jarnik 构造出了一个适合前述条件的函数, 而在曲线

$$v=f(u), \quad \frac{1}{2}\leqslant u\leqslant w$$

上有多于 cz^2 个整点.

7.4　圆内整点问题与除数问题

用 $r(n)$ 表示将非负整数 n 分解成两个平方之和的分法种数. 和数 $A(x)=\sum_{0\leqslant n\leqslant x} r(n)$ 就等于落在圆 $u^2+v^2\leqslant x$ 中的整点 (u,v) 的个数. Gauss[66] 首先证明了

$$A(x)=\pi x+O(\sqrt{x}). \tag{122}$$

以后, Jarnik[240] 推广了他的证明原则, 而证明了下面的一般结果: 设 D 为一封闭的有长 Jordan 曲线, L 为它的长, A 为它所围的面积, 而 N 为含在 D 内的整点个数, 则有

$$|A-N|<L.$$

现在人们把寻求使 (122) 成立的最佳误差项的问题称做圆内整点问题.

设 $d(n)$ 为 n 的因子个数. 和数 $D(x)=\sum_{1\leqslant n\leqslant x} d(n)$ 就等于包含在双曲线的扇形

$$uv\leqslant x,\quad u\geqslant 1,\quad v\geqslant 1$$

中的整点 (u,v) 的个数. Dirichlet[67] 首先证明:

$$D(x)=x(\log x+2\gamma-1)+O(\sqrt{x}), \tag{123}$$

此处 γ 表 Euler 常数. 寻求使 (123) 成立的最佳误差项的问题称为除数问题.

寻求使表示式 (122) 与 (123) 成立的最佳误差项的问题, 吸引了几何数论方面的研究工作者的主要注意力.

1903 年, Вороной[241] 首先打破记录, 他对除数问题得到了用 $O(x^{\frac{1}{3}}\log x)$ 代替 $O(x^{\frac{1}{2}})$ 的结果; 而在 1906 年, Sierpinski[242] 对圆内整点问题, 成功地用 $O(x^{\frac{1}{3}})$ 代替了 $O(x^{\frac{1}{2}})$.

7.5　估计指数和的方法

用 ϑ 表示使

$$A(x)=\pi x+O(x^{\nu})$$

成立的 ν 的下极限. van der Corput 引进了估计指数和的方法, 从而证明了比 $\vartheta\leqslant\dfrac{1}{3}$ 更好的结果. 这个结果已为很多数学工作者改进. ϑ 的历史可以总结如下表:

$\vartheta \leqslant$	1/3	37/112	37/112	
作者姓名	W. Sierpinski	J. G. van der Corput[34]	J.E.Littlewood[248] 与 A.Walfisz	
$\vartheta \leqslant$	163/494	27/82	15/46	13/40
作者姓名	A. Walfisz[244]	L. W. Nieland[245]	E. C. Titfchmarsh[78]	华罗庚[246]

除数问题的对应发展如下：

$\vartheta \leqslant$	1/3	33/100	27/82	15/46
作者姓名	Г. Ф. Вороной	J. G. van der Corput[74]	J. G. van der Corput[247]	迟宗陶[245] H. E. Richert[240]

另一方面, 对于这两种情形, Hardy[250] 与 Ingham[251] 证明了 $\vartheta \geqslant \frac{1}{4}$, 或者更精确地有

$$\varlimsup_{x\to\infty}\frac{A(x)-\pi x}{x^{\frac14}\log^{\frac14}x}>0,\ \varliminf_{x\to\infty}\frac{A(x)-\pi x}{x^{\frac14}\log^{\frac14}x}<0$$

及

$$\varliminf_{x\to\infty}\frac{D(x)-x\log x-(2\gamma-1)x}{x^{\frac14}\log^{\frac14}x\log\log x}<0<\varlimsup_{x\to\infty}\frac{D(x)-x\log x-(2\gamma-1)x}{x^{\frac14}\log^{\frac14}x\log\log x}.$$

关于误差项的均值, 我们有下面的定理:

$$\int_0^x (A(y)-\pi y)^2\mathrm{d}y=\frac{1}{3\pi^2}\frac{16\zeta^3\left(\frac32\right)L^2\left(\frac32\right)}{\zeta(3)(1+2^{-\frac32})}x^{\frac32}+O(x^{1+\varepsilon})^{252)}$$

及

$$\int_0^x (D(y)-y\log y-(2\gamma-1)y)^2\mathrm{d}y=cx^{3/2}+O(x\log^5 x)^{253)}.$$

7.6　除数问题的推广

用 $d_k(n)$ 表示将 n 表成 k 个因子乘积的表法种数, 又命

$$D_k(x)=\sum_{n\leqslant x}d_k(n),$$

则有

$$D_k(x)=\frac{1}{2\pi\mathrm{i}}\int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty}\zeta^k(w)\frac{x^w}{w}\mathrm{d}w,\quad c>1.$$

$w=1$ 为一 k 次极点, 其上的留数形如 $xP_k(\log x)$, 此处 P_k 为一 $k-1$ 次多项式. 我们记

$$D_k(x)=xP_k(\log x)+\Delta_k(x).$$

对于 $k=2$, 我们回到了上面研究过的除数问题. 我们相应地定义 α_k 为使

$$\Delta_k(x)=O(x^{\vartheta})$$

成立的数 ϑ 的下极限, 它的历史一览表如下：

$$\alpha_k \leqslant \frac{k-1}{k+1},\quad k=2,3,4,\cdots \quad (\text{Вороной}^{241)}, \text{Landau}^{238)}),$$

$$\alpha_k \leqslant \frac{k-1}{k+2},\quad k=4,5,\cdots \quad (\text{Hardy-Littlewood}^{254)}),$$

$$\alpha_7 \leqslant \frac{71}{107},\quad \alpha_8 \leqslant \frac{41}{59},\quad \alpha_9 \leqslant \frac{31}{43},\quad \alpha_{10} \leqslant \frac{26}{35},\quad \alpha_{11} \leqslant \frac{19}{25} \quad (\text{董光昌}^{255)}),$$

$$\alpha_3 \leqslant \frac{37}{75} \quad (\text{Atkinson}^{255)}),$$

$$\alpha_k \geqslant \frac{k-1}{2k} \quad (\text{Hardy}^{250)}).$$

猜想的结果是

$$\alpha_k=\frac{k-1}{2k}.$$

用 β_k 表示 $\Delta_k(x)$ 的平均阶, 亦即对任何 $\varepsilon>0$, 使

$$\frac{1}{x}\int_0^x \Delta_k^2(y)\mathrm{d}y=O(x^{2\beta_k+\varepsilon})$$

成立的最小的数. 显然有

$$\beta_k \leqslant \alpha_k.$$

Titchmarsh[257] 证明了

$$\beta_k \geqslant \frac{k-1}{2k}.$$

又, 人们已经证明：

$$\beta_3=\frac{1}{3} \quad (\text{Cramér}^{258)}),\quad \beta_4 \leqslant \frac{23}{54} \quad (\text{董光昌}^{255)}),\quad \beta_5 \leqslant \frac{1}{2}^{255)},$$

$$\beta_6 \leqslant \frac{35}{62}^{255)},\quad \beta_7 \leqslant \frac{11}{18}^{255)} \quad \text{及} \quad \beta_8 \leqslant \frac{149}{230}^{255)}.$$

7.7　圆内整点问题的推广

我们研究 n 维椭球

$$F(u_1,\cdots,u_n)=\sum_{\mu,\nu=1}^{n} a_{\mu\nu}u_\mu u_\nu,\quad a_{\mu\nu}=a_{\nu\mu}$$

中的整点个数 $A(x)=A_F(x)$, 此处 $F(u_1,\cdots,u_n)$ 为一具有行列式 D 的正定二次型. 如果存在数 $\alpha(\neq 0)$, 使对全体 $\mu,\nu,\alpha a_{\mu\nu}$ 都是整数, 则称型 F 为有理的; 否则称 F 为无理的.

用 $V(x)=V_F(x)$ 表示椭球

$$F(u_1,\cdots,u_n)\leqslant x$$

的体积, 大家知道

$$V(x)=\pi^{\frac{n}{2}}x^{\frac{n}{2}}\Big/\sqrt{D}\Gamma\left(\frac{n}{2}+1\right).$$

命

$$P(x)=A_Q(x)-V_Q(x),$$

Landau[259] 证明了

$$P(x)=O(x^{\frac{n}{2}-\frac{n}{n+1}}),$$
$$P(x)=\Omega(x^{\frac{n-1}{4}}).$$

对于 $n\geqslant 8$, 关于有理型 F 的 O- 问题, 已为 Walfisz[260] 完全解决. 对于 $4\leqslant n\leqslant 7$, Landau[261] 用 Walfisz 方法的一个变形, 得到了阶中指数的最优结果. 这就是: 如果 F 为有理, 则

$$P(x)=O(x^{\frac{n}{2}-1}),\quad n>4,$$
$$P(x)=O(x\log^2 x),\quad n=4.$$

Jarnik[262] 证明了

$$P(x)=\Omega(x^{\frac{n}{2}-1}).$$

对于 $n=4$, Landau 获得的结果与最后结果只相差一个对数因子. 下面是更精确的结果:

$$P(x)=O(x\log^{\frac{4}{5}}x\log\log x)\quad (\text{Walfisz}^{263)}),$$
$$P(x)=O(x\log^{\frac{2}{3}+\varepsilon}x)^{264)}.$$

设

$$R(x)=\frac{1}{x}\int_0^x|P(y)|\mathrm{d}y,$$
$$T(x)=\left(\frac{1}{x}\int_0^x P^2(y)\mathrm{d}y\right)^{\frac{1}{2}},$$

Jarnik[262] 证明了

a) $$R(x)=\Omega(x^{\frac{n-1}{4}}).$$

b) 对于有理型 F,

$$R(x)=\Omega(x^{\frac{n}{2}-1}).$$

c) 对于 $F=\sum_{i=1}^{n}\alpha_i x_i^2$,

$$\begin{aligned}
&R(x)=O(x^{\frac{1}{4}}\log^2 x),\quad n=2,\\
&R(x)=O(x^{\frac{1}{2}}\log x),\quad n=3,\\
&R(x)=O(x^{\frac{n}{2}-1}),\quad n>3.
\end{aligned}$$

d) 如果将 $R(x)$ 换成 $T(x)$, 上列结果仍然正解.

Jarnik[265] 证明: 如果 F 的全体系数 $a_{\mu\nu}$ 都是整数, 则有一仅依于 F 的 H, 使

$$\int_0^x P^2(y)\mathrm{d}y=\begin{cases} Hx^2\log x+O(x^2\log^{\frac{1}{2}}x), & n=3,\\ Hx^{n-1}+O(g(x)), & n>3,\end{cases}$$

此处

$$\begin{aligned}
&g(x)=x^{\frac{5}{2}}\log x,\quad n=4,\\
&g(x)=x^3\log^2 x,\quad n=5,\\
&g(x)=x^{n-2},\quad n>5.
\end{aligned}$$

对于 $n>5$, 上之结果已是可能得到的最优结果. 对于 $n=4$, Walfisz 也得到了此同一结果. Walfisz 也讨论了和数

$$\sum_{m\leqslant x}r^2(m),$$

此处 $r(m)$ 为 $F=n$ 的整数解数. 有关这些问题的结果的详尽叙述, 可在 Walfisz 的标题为 "高维椭球中的整点问题 I—IX" 的原始工作中找到.

Jarnik 还研究了椭球

$$F=\alpha_1(x_1^2+\cdots+x_\nu^2)+\alpha_2(x_{\nu+1}^2+\cdots+x_n^2).$$

对于 $n=3$, $F=x_1^2+x_2^2+x_3^2$, 这就是所谓球内整点问题. 我们用 $x_1=x_2$, $x_2=x_3$, $x_3=x_1$; $x_1=0$, $x_2=0$ 与 $x_3=0$ 等六个平面将球分成 48 个部分, 在每一部分中的整点个数显然相等, 我们用 G 表示此数. 截面上的整点都以半数计之, 于是因为截面交线上的整点个数等于 $O(\sqrt{x})$, 故有

$$A=48G+O(x^{\frac{1}{2}}).$$

显然

$$\begin{aligned}
G=&\sum_{0<x_1\leqslant\frac{x^{\frac{1}{2}}}{\sqrt{3}}}\ \sum_{x_1<x_2\leqslant\sqrt{\frac{1}{2}(x-x_1^2)}}[\sqrt{x-x_1^2-x_2^2}-x_2]+\frac{1}{2}\sum_{0<x_2\leqslant\frac{x^{\frac{1}{2}}}{\sqrt{2}}}([\sqrt{x-x_2^2}]-x_2)\\
&+\frac{1}{2}\sum_{0<x_1\leqslant\frac{x^{\frac{1}{2}}}{\sqrt{3}}}([\sqrt{x-2x_1^2}]-x_1)+\frac{1}{2}\sum_{0<x_1\leqslant\frac{x^{\frac{1}{2}}}{\sqrt{3}}}\left(\left[\sqrt{\frac{1}{2}(x-x_1^2)}\right]-x_1\right)+O(x^{\frac{1}{2}}).
\end{aligned}$$

在建立了 [75]Fourier 级数与函数的分数部分间的一个关系后, Виноградов依靠 van der Corput 引理 (第二章, §8) 的帮助, 证明了

$$P(x)=O(x^{0.7+\varepsilon})\quad(\text{Виноградов}^{266)}),$$
$$P(x)=O(x^{0.7-\frac{1}{405}+\varepsilon})\quad(\text{Виноградов}^{267)}),$$
$$P(x)=O(x^{\frac{11}{16}+\varepsilon})\quad(\text{Виноградов}^{268)}).$$

又 Szegö[269] 证明了

$$P(x)=\Omega(x^{\frac{1}{2}}\log^{\frac{1}{2}}x).$$

Виноградов估计球内整点个数的方法, 可以直接用来估计具有负判别式 $-t$ 而 $t\leqslant x$ 的纯虚二次型的全体类数之和. 事实上, 这两问题的相互关系类似于二维空间中的圆内整点问题与除数问题的关系.

对于球面上的整点个数的估计, Линник[270] 得到下面的

定理 设 $m=1,2(\mathrm{mod}\ 4)$ 或 $m=3(\mathrm{mod}\ 8)$; 又设 Γ 为球 $F_3: x^2+y^2+z^2=m$ 上的一个凸球面区域, 它的边界由有限多条光滑曲线组成. 用 q 表一适合条件 $\left(\dfrac{-m}{q}\right)=1$ 的奇素数. 命 $H_0(m)$ 与 $H_0(\Gamma)$ 分别表示 F_3 上的与 Γ 中的适合 $(x,y,z)=1$ 的整点个数, 又命 $H(m)$ 与 $H(\Gamma)$ 分别表示 F_3 上的与 Γ 中的整点个数, 则对固定的 q 与 $m\to\infty$, 可有

$$H_0(\Gamma)=\frac{\mathrm{mes}\ \Gamma}{4\pi m}H_0(m)(1+K_0(\lambda,m,q)),$$
$$H(\Gamma)=\frac{\mathrm{mes}\ \Gamma}{4\pi m}H(m)(1+K(\lambda,m,q)),$$

此处 mes Γ 表 Γ 的面积; $\lambda>0$ 为适合 $\dfrac{\mathrm{mes}\ \Gamma}{4\pi m}>\lambda$ 的任何常数, 而对固定的 λ,q 及 $m\to\infty$, 有 $K_0(\lambda,m,q)\to 0$ 及 $K(\lambda,m,q)\to 0$.

Малышев[271] 将上述结果推广到某种椭球.

7.8 无 k 方因子数的分布

如果一个整数不能被任何大于 1 的整数的 k 次乘幂所整除, 就称它为一无 k 方因子的整数. 用 $Q_k(x)$ 表示 $\leqslant x$ 的无 k 方因子整数的个数, 则

$$\begin{aligned}Q_k(x)&=\sum_{l^k m\leqslant x}\mu(l)=\sum_{l\leqslant x^{\frac{1}{k}}}\mu(l)\left[\frac{x}{l^k}\right]=x\sum_{l\leqslant x^{\frac{1}{k}}}\frac{\mu(l)}{l^k}+O(x^{\frac{1}{k}})\\&=\zeta^{-1}(k)x+O(x^{\frac{1}{k}}).\end{aligned}$$

这儿的误差项可用第三章 §19 的方法加以改进.

又用 $q_k(n)$ 表示第 n 个无 k 方因子数, 则当 $n\to\infty$ 时, 显然有 $q_k(n)\sim\zeta^{-1}(k)n$. Fogels[141] 证明了

$$q_k(n+1)-q_k(n)=O(n^{\frac{k}{3k-1}+\varepsilon}).$$

这个结果被下述的 Davenport 与 Roth[272] 的结果所代替. 对于任何 $t>1$, 我们有

$$\begin{aligned}Q_k(x+h)-Q_k(x)&=\sum_{x<l^km\leqslant x+h}\mu(l)\\&=\sum_{1\leqslant l\leqslant t}\mu(l)\left(\left[\frac{x+h}{l^k}\right]-\left[\frac{x}{l^k}\right]\right)+O(\sum_{\substack{x<l^km\leqslant x+h\\ l>t}}1)\\&=\frac{h}{\zeta(k)}+O(t)+O(ht^{1-k})+O(N),\end{aligned}$$

这里的 N 表示适合 $x<l^km\leqslant x+h, l>t$ 的数对 (l,m) 的对数. 关于 N 的估计为

$$O(x^{\frac{1}{2k-1}+\varepsilon}(ht^{-\frac{2k}{2k-1}}+t^{-\frac{1}{2k-1}})).$$

于是

$$q_k(n+1)-q_k(n)=O(n^{\frac{1}{2k}+\varepsilon}).$$

对于 $k=2$, 这个结果已用 van der Corput 关于指数和的估计加以改善, 它的最新结果属于 Richert[273], 此即

$$q_2(n+1)-q_2(n)=O(n^{\frac{2}{9}}\log n).$$

Erdös[274] 给出它的下估计, 他证明了

$$q_2(n+1)-q_2(n)=\Omega\left(\frac{\log n}{\log\log n}\right).$$

7.9 一 般 方 法

Cauchy 积分定理在一般数论问题中的应用源于 Landau[238] 的一个工作. 在这工作中, 他证明了下面的

定理　假设: c_ν, l_ν 都是复数; $\alpha\geqslant 0, \alpha_i, \gamma_i$ 为实数; δ_i, β_i 都是正数; μ 与 ν 是 $\geqslant 1$ 的整数; $\lambda_1<\lambda_2<\cdots<\lambda_n<\cdots$:

a) 对于任何 $\varepsilon>0$, 都有

$$c_n=O(n^{\alpha+\varepsilon});$$

b) 对于 $\sigma>1+\alpha$, 由

$$Z(s)=\sum_{n=1}^{\infty}\frac{c_n}{n^s}$$

定义的函数在全平面上是半纯的, 且在任何带状区域 $\sigma_1 \leqslant \sigma \leqslant \sigma_2$ 中有有限多个极点;

c) $$\sum_{n=1}^{\infty} l_n \mathrm{e}^{\lambda_n s}$$

在 $\sigma < 0$ 时绝对收敛;

d) 对于 $\sigma < 0$,

$$\begin{aligned} &\Gamma(\alpha_1 + \beta_1 s) \cdots \Gamma(\alpha_\mu + \beta_\mu s) Z(s) \\ &= \Gamma(\gamma_1 - \delta_1 s) \cdots \Gamma(\gamma_\nu - \delta_\nu s) \sum_{n=1}^{\infty} l_n \mathrm{e}^{\lambda_n s}; \end{aligned}$$

e) $$\beta_1 + \cdots + \beta_\mu = \delta_1 + \cdots + \delta_\nu;$$

f) 如命

$$\gamma_1 + \cdots + \gamma_\nu - (\alpha_1 + \cdots + \alpha_\mu) + \frac{1}{2}(\mu - \nu) = \eta,$$

则有

$$\eta \geqslant \frac{1}{2} \quad 及 \quad \eta \geqslant \alpha + \frac{1}{2};$$

g) 对于固定的带状区域 $\sigma_1 \leqslant \sigma \leqslant \sigma_2$, 存在常数 $\gamma = \gamma(\sigma_1, \sigma_2)$, 使对 $\sigma_1 \leqslant \sigma \leqslant \sigma_2$ 及大的 $|t|$, 有

$$Z(s) = O(\mathrm{e}^{\gamma |t|})$$

成立.

结论 对于任何 $\varepsilon > 0$, 有

$$\sum_{n \leqslant x} c_n = R(x) + O(x^{(\alpha+1)\frac{2\eta-1}{2\eta+1}+\varepsilon}),$$

此处 $R(x)$ 为在带状区域

$$(\alpha+1)\frac{2\eta-1}{2\eta+1} < \sigma \leqslant \alpha + 1$$

中的 $\dfrac{Z(s)}{s}$ 的一切可能的极点上函数

$$\frac{x^s}{s} Z(s)$$

的各个留数之和.

由上面的定理, Landau 立刻得到下述结果:

$$\sum_{n \leqslant x} D_k(n) = x(b_{k-1} \log^{k-1} x + \cdots + b_0) + O(x^{\frac{k-1}{k+1}+\varepsilon}), \quad k \geqslant 2,$$

$$\sum_{\sum\limits_{1 \leqslant \mu, \nu \leqslant k} a_{\mu\nu} u_\mu u_\nu \leqslant x} 1 = I x^{\frac{k}{2}} + O(x^{\frac{k-1}{2}\frac{k}{k+1}+\varepsilon}), \quad k \geqslant 2,$$

这里的 $\sum\limits_{1\leqslant\mu,\nu\leqslant k} a_{\mu\nu}u_\mu u_\nu$ 为一正定型, 而 $Ix^{\frac{k}{2}}$ 表示 $\sum\limits_{1\leqslant\mu,\nu\leqslant k} a_{\mu\nu}u_\mu u_\nu \leqslant x$ 的体积. 又

$$\sum_{Na\leqslant x} 1 = \alpha x + O(x^{\frac{1}{3}+\varepsilon}),$$

此处 Na 表示虚二次域 K 中的理想数 a 的距.

命 $\chi_1(n), \cdots, \chi_k(n)$ 为 k 个非主特征, 则有

$$\sum_{n_1\cdots n_k\leqslant x} \chi_1(n_1)\cdots\chi_k(n_k) = O(x^{\frac{k-1}{k+1}+\varepsilon}).$$

如果在 $\chi_1(n), \cdots, \chi_k(n)$ 中有主特征, 则此结果仍然正确, 但在右方多添一主项.

重要问题索引

问题	结果	作者	发表年代	
密率问题	假如两个集合的密率之和大于或等于 1, 则和集的密率等于 1.	Schnirelmann	1930	§1.1
	假如两个集合的密率之和小于 1, 则和集的密率大于或等于这两集合密率的和.	Mann	1942	§1.1
Kloostermann 和	若 $(c,p)=1$, 则 $\left\lvert\sum_{x=1}^{p-1} \mathrm{e}^{2\pi\mathrm{i}(cx+\frac{d}{x})/p}\right\rvert \leqslant 2\sqrt{p}$.	Weil	1948	§2.6
完全指数和	设 p 为一素数, $f(x)=a_kx^k+\cdots+a_1x$, 又设 $p\nmid a_k$, 则 $\left\lvert\sum_{x=1}^{p} \mathrm{e}^{2\pi\mathrm{i}f(x)/p}\right\rvert \leqslant k\sqrt{p}$.	Weil-Carlitz-Uchiyama	1957	§2.6
	设 q 为一 $\geqslant 1$ 的整数, 又 $f(x)=a_kx^k+\cdots+a_1x$ 为一 k 次整系数多项式, 并且 $(a_k,\cdots,a_1,q)=1$, 则有 $\left\lvert\sum_{x=1}^{q} \mathrm{e}^{2\pi\mathrm{i}f(x)/q}\right\rvert \ll q^{1-\frac{1}{k}+\varepsilon}$, 记号 $\ll$ 中所含的常数与 ε 及 k 有关.	华罗庚	1940	§2.7
mod p 的幂剩余	设 n 是 $p-1$ 的一个因子, 它不等于 1, 则对全体充分大的 p, mod p 的最小正 n 次非剩余 $< p^{\frac{1}{2k}}(\log\ p)^2, k=\mathrm{e}^{\frac{n-1}{n}}$.	Виноградов	1926	§2.8
mod p 的原根	用 $g(p)$ 表示 p 的最小正原根, 则有 $g(p)=O(2^{m+1}\sqrt{p})$, 此处 m 为 $p-1$ 的互不相同的素因子个数.	华罗庚	1942	§2.8
素数分布	设 $\pi(x;q,l)$ 为等差级数 $qn+l$ 中不大于 x 的素数个数, 则有 $\pi(x;q,l)=\frac{\mathrm{li}\ x}{\varphi(q)}+O(x\mathrm{e}^{-c(\log\ x)^{\frac{3}{5}-\varepsilon}})$, 记号 O 中的常数与 q 及 ε 有关.	Виноградов	1958	§3.4 §3.7
	对于 $q\leqslant(\log\ x)^u, u$ 为任意一数, 可有 $\pi(x;q,l)=\frac{\mathrm{li}\ x}{\varphi(q)}+O(x\mathrm{e}^{-c\sqrt{\log\ x}})$, 记号 O 中所含的常数关于 q 为一致.	Page-Siegel-Walfisz-	1936	§3.7
	落在区间 $(A,A+x)$ 中的素数个数 $\leqslant\frac{2x}{\log\ x}+O\left(\frac{x}{\log^2 x}\cdot\log\log\ x\right)$, 记号 O 中所含的常数关于 A 为一致.	Selberg	1947	§1.4
	等差级数 $\equiv l(\mathrm{mod}\ q)$ 中的最小素数等于 $Q(q^C)$, 此处 C 为一绝对常数.	Линник	1944	§3.7
	$\pi(x)-\mathrm{li}\ x=\Omega\left(\frac{x^{\frac{1}{2}}}{\log\ x}\log\log\log\ x\right)$.	Littlewood	1914	§3.5
相继素数的差距	用 p_n 表第 n 个素数, 则 $p_{n+1}-p_n=O(p_n^{\frac{38}{61}+\varepsilon})$.	Ingham	1937	§3.6

续

问题	结果	作者	发表年代	
	对于任何 $\varepsilon > 0$, 有无限多个 n, 使 $p_{n+1} - p_n \geqslant \left(\frac{1}{3} - \varepsilon\right) \log p_n \cdot \log\log p_n \frac{\log\log\log\log p_n}{(\log\log\log p_n)^2}$	Rankin	1938	§3.6
	对于任何 $\varepsilon > 0$, 有无限多个 n, 使 $p_{n+1} - p_n \leqslant \left(\frac{57}{59} + \varepsilon\right) \log p_n.$	Rankin	1940	§3.6
Waring 问题	用 $G(k)$ 表示最小的整数 s 之能使任何大整数都可表成至多 s 个 k 次乘幂之和者, 则 $G(k) \leqslant k(3\log k + 9)$, $G(3) \leqslant 7$, $G(4) = 16, G(5) \leqslant 23, G(6) \leqslant 36.$	 Виноградов Линник Davenport	 1947 1942 1939	 §4.2 §4.2 §4.2
	用 $g(k)$ 表示最小的整数 s 之能使任何整数都可表成至多 s 个 k 次乘幂之和者, 则在 $\left(\frac{3}{2}\right)^k - \left[\left(\frac{3}{2}\right)^k\right] \leqslant 1 - \left(\frac{1}{2}\right)^k \left\{\left[\left(\frac{3}{2}\right)^k\right] + 3\right\}$ 成立时, $g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2, \quad k > 6.$	Dickson-Pillai-Niven	1936–1944	§4.4
	$g(6) = 73$, $19 \leqslant g(4) \leqslant 35, \quad 37 \leqslant g(5) \leqslant 54$, $g(3) = 9$, $g(2) = 4$	Pillai Dickson Wieferich Lagrange	1940 1933 1909 1770	§4.4 §4.4 Math.Ann. **66**, 95–101, 1909. 见 L. E. Dickson著 History of the theory of numbers II (New York) 275–304, 1934.
	当 $s \geqslant \begin{cases} 2k+1, & 1 \leqslant k \leqslant 10, \\ 2k^2(2\log k + \log\log k + 2.5), & k > 10 \end{cases}$ 时, 能够得到方程 $N = x_1^k + \cdots + x_s^k$ 的解数的渐近公式.	华罗庚	1953	§4.1

续

问题	结果	作者	发表年代	
Prouhet 问题	用 $N(k)$ 表示具有下面性质的最小的 t: 存在 $x_1,\cdots,x_t,y_1,\cdots,y_t$, 但 $y_1,\cdots,y_t$ 并非 $x_1,\cdots,x_t$ 的重新排列, 它们满足 $\sum\limits_{i=1}^{t} x_i^h=\sum\limits_{i=1}^{t} y_i^h,\quad 1\leqslant h\leqslant k.$ 则有 $N(k)\leqslant\begin{cases}\frac{1}{2}(k^2+3), & 若\ 2\nmid k,\\ \frac{1}{2}(k^2+4), & 若\ 2\mid k.\end{cases}$	Wright	1935	§4.5
	用 $M(k)$ 表示使 $\sum\limits_{i=1}^{t} x_i^h=\sum\limits_{i=1}^{t} y_i^h,\quad 1\leqslant h\leqslant k,$ $\sum\limits_{i=1}^{t} x_i^{k+1}\neq\sum\limits_{i=1}^{t} y_i^{k+1}$ 可解的最小的 t, 则 $M(k)\leqslant(k+1)\left(\left[\frac{\log\frac{1}{2}(k+2)}{\log(1+\frac{1}{k})}\right]+1\right).$	华罗庚	1938	§4.5
	$M(k)=k+1,\quad 2\leqslant k\leqslant 9.$			A. Gloden, Mehrgradige Gleichungen, Groningen 1944.
Goldbach 问题 275)	每一大奇数都是三个素数的和.	Виноградов	1937	§2.9 §5.1
	每一大偶数都是一个素数与一个是有限多个素数乘积的数之和.	Rényi	1947	§5.3
	每一大偶数都是两个乘积数之和, 其中一个不超过两个素数的乘积, 而另一个则不超过 366 个素数的乘积.	Ricci	1937	§1.3
Waring-Goldbach 问题	当 $s\geqslant\begin{cases}2^k+1, & 1\leqslant k\leqslant 10,\\ 2k^2(2\log k+\log\log k+2.5), & k>10\end{cases}$ 时, 能够得到方程 $N=p_1^k+\cdots+p_s^k$ 的解数的渐近公式, 这里的 p_i 都是素数.	华罗庚	1953	§3.4
	用 $H(k)$ 表示具有以下性质的最小整数 s; 每一充分大的整数 (适合某些条件的) 都是 s 个素数的 k 次乘幂之和, 则 $H(k)\leqslant c(k)\sim 4k\log k,$ $H(4)\leqslant 15, H(5)\leqslant 25, H(6)\leqslant 37,$ $H(7)\leqslant 55, H(8)\leqslant 75.$	华罗庚	1953	§3.4

续

问题	结果	作者	发表年代	
圆内整点问题	对于圆 $u^2+v^2\leqslant x$ 中的整点 (u,v) 的个数 $A(x)$, 有 $A(x)=\pi x+O(x^{\frac{13}{40}+\varepsilon})$	华罗庚	1942	§7.5
	$\varliminf\limits_{x\to\infty}\frac{A(x)-\pi x}{x^{\frac14}\log^{\frac14}x}<0<\varlimsup\limits_{x\to\infty}\frac{A(x)-\pi x}{x^{\frac14}\log^{\frac14}x}$	Hardy	1916	§7.5
	$\int_0^x(A(y)-\pi y)^2\mathrm{d}y=\frac{1}{3\pi^2}\cdot\frac{16\zeta^2\left(\frac32\right)L^2\left(\frac32\right)}{\zeta(3)(1+2^{-\frac32})}x^{\frac32}+O(x^{1+\varepsilon})$.	Landau	1924	§7.5
除数问题	用 $D(x)$ 表示双曲扇形 $uv\leqslant x,u\geqslant 1,v\geqslant 1$ 中的整点 (u,v) 的个数, 则有 $D(x)=x(\log x+2\gamma-1)+O(x^{\frac{15}{46}+\varepsilon})$.	迟宗陶, Richert	1950	§7.5
	$\int_0^x(D(y)-y(\log y+2\gamma-1))^2\mathrm{d}y=cx^{\frac32}+O(x\log^5 x)$.	董光昌	1956	§7.5
	$\varliminf\limits_{x\to\infty}\frac{D(x)-x(\log x+2\gamma-1)}{x^{\frac14}\log^{\frac14}x\log\log x}<0<\varlimsup\limits_{x\to\infty}\frac{D(x)-x(\log x+2\gamma-1)}{x^{\frac14}\log^{\frac14}x\log\log x}$.	Hardy	1916	§7.5
球内整点问题	对于落在球 $u^2+v^2+w^2\leqslant x$ 中的整点 (u,v,w) 的个数 $P(x)$, 有 $P(x)=\frac43\pi x^{\frac32}+O(x^{\frac{11}{16}+\varepsilon})$.	Виноградов	1955	§4.7
椭球内的整点问题	设 $F(u_1,\cdots,u_n)=\sum\limits_{\mu,\nu=1}^{n}a_{\mu\nu}u_\mu u_\nu$ 为一有行列式 D 的正定型. 如果存在 $\alpha(\neq 0)$, 使对全体 μ 与 $\nu,\alpha a_{\mu\nu}$ 都是整数, 则对 $n\geqslant 8$, 有 $\sum\limits_{F(u_1,\cdots,u_n)\leqslant x}1=\frac{\pi^{\frac n2}x^{\frac n2}}{\sqrt{D}\Gamma(\frac n2+1)}+O(x^{\frac n2-1})$.	Walfisz	1924	§4.7
	在上面的假定下, 此同一结论对 $5\leqslant n\leqslant 7$ 也成立.	Landau	1924	§4.7
	在上面的假定下, 有 $\sum\limits_{F(u_1,\cdots,u_n)\leqslant x}1=\frac{\pi^{\frac n2}x^{\frac n2}}{\sqrt{D}\Gamma(\frac n2+1)}=\Omega(x^{\frac n2-1})$.	Jarnik	1931	§4.7

参考书籍

H. Bohr und H. Cramér, Die neuere Entwicklung der analytischen Zahlentheorie, Enzyklopädie der mathematischen Wissenschaften mit Einschluß ihrer Anwendungen II, 3, b, Leipzig, 1923–1927.

T. Estermann, Introduction to modern prime number theory, Cambridge tracts, Cambridge University Press, **41**, 1952.

А. О. Гельфонд, Трансцендентные и алгебраические числа, ГИТТЛ., Москва, 1952.

华罗庚, 堆垒素数论, 科学出版社, 1953. (新版, 1957. 有俄文本; Аддитивная теория простыхчисел, Тр. Матем. ин-та. нм. В. А. Стеклова АН СССР, 1947, т. XXП).

I. F. Koksma, Diophantische Approximationen, Springer Verlag, Berlin, 1936.

A. E. Ingham, The distribution of prime numbers, Cambridge tracts, Cambridge University Press, **30**, 1932.

E. Landau, Handbuch der Lehre von der Verteilung der Primzahlen, 1 und 2, Leipzig und Berlin, 1909.

E. Landau, Über einige neuere Fortschritte der additiven Zahlentheorie, Cambridge tracts, Cambridge University Press, **35**, 1937.

E. Landau, Vorlesungen Über Zahlen-theorie, Bd, I. II, III, Leipzig, 1927.

E. Landau, Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale, 2. Aufl., Leipzig 1927.

H. H. Ostmann, Additive Zahlentheorie, Bd, I. II, Springer-Verlag, Berlin, 1956.

K. Prachar, Primzahlverteilung, Springer Verlag, Berlin-Göttingen-Heidelberg, 1957.

C, L. Siegel, Transcendental numbers, Princeton Univ. Press, 1949.

Н. Г. Чудаков, Введение в теорию *L*-функций дирихле, ГИТТЛ; Москва-Ленинград, 1947.

E. C. Titchmarsh, The theory of the Riemann Zeta function, Clarendon Press, Oxford, 1951.

P. Turán, Eine neue Methode in der Analysis und deren Anwendungen, Akadémiai Kiadó, Budapest, 1953 (有中译本: "数学分析中的一个新方法及其应用", 郭焕庭译, 见数学进展, 2 卷, 312–365, 1956).

И. М. Виноградов, Избранные труды, Изд. АН СССР, Москва, 1952.

И. М. Виноградов, Метод тригонометрических сумм в теории чисел, Тр. Матем. ин-таим. В. А. Стеклова, АН СССР, 1947, XXШ, (有中译本: "数论中的三角和法". 越民义译, 见数学进展, 一卷一期, 3–106, 1955; 英译本: The method of trigonometrical sums in the theory of numbers, K. F. Roth 与 A. Davcnport 译, Interscience publishers, London-Now York, 1954).

A. Walfisz, Gitterpunkte in mehrdimensionalen Kugeln, Warszawa, 1957.

参考资料

[1] L. E. Dickson, History of the theory of numbers, New York, **1**, 421, 1934.

[2] N. Pipping 核对了命题 (A) 当$N \leqslant 10^5$ 是正确的.

[3] E. Landau, Gelöste und ungelöste Probleme aus der Theorie der Primzahlverteilung und der Riemannschen Zetafunktion, Proc. of the 5th Inter. Congress of Math., Cambridge, **1**, 93–108, 1912.

[4] E. Waring, Meditationes algebraicae, Cambridge, 204–205, 1770, 亦见 L. E. Dickson, History of the theory of numbers, New York, **2**, 717–729, 1934.

[5] D. Hilbert, Beweis für die Darstellbarkeit der Ganzen Zahlen durch eine feste Anzahl n-ter Potenzen, Math. Ann., **67**, 281–300, 1909.

[6] Л. Г. Шнирельман, об аддитивных свойствах чисел, Ростов Н/Д, Изв. Донск. Политехн. ин-та. 14: 2–3 (1930), 3–28; Über additive Eigenschaften von Zahlen, Math. Ann., **107**, 649–690, 1933.

[7] G. H. Hardy und J. E. Littlewood, Some problems of "Partitio numerorum"; I: A new solution of Waring's Problem, Gött. Nachr, 33–54, 1920; II. Proof that every large number is the sum of at most 21 biquadrates, Math. Z., **9**, 14–27, 1921; III: On the expression of a number as a sum of primes, Acta Math., **44**, 1–70, 1922, IV: The singular series in Waring's Problem and the value of the number G(k), Math. Z., **12**, 161–188, 1922; V. A further contribution to the study of Goldbach's problem, Proc. London Math. Soc. (2); **22**, 46–56, 1923. VI: Further Researches in Waring's Problem, Math. Z., **23**, 1–37. 1925, VII: The number $\Gamma(k)$ in Waring's Problem, Proc. London Math. Soc., **28**, 518–542, 1928.

[8] 事实上, 这个方法的思想已经在 Hardy 与 Ramanujan 的下述论文中出现过: "Asymoptotic formulae in combinatory analysis", Proc. London Math. Soc. (2), **17**, 75–115, 1918.

[9] E. Landau, Vorlesungen Über Zahlentheorie, Leipzig, **1**, 183–234, 1927.

[10] И. М. Виноградов, Представление нечётного числа суммой трёх простых чисел, ДАН СССР, **15**, 291–294, 1937.

[11] К. Г. Бороздкий, К Вопросу о постоянной И. М. Виноградова, Тру. Тре. Всесо юзного Матем. Съезда, СССР, **1**, **3**, 1956.

[12] Ю. Б. Линник, О густоте нулей L-рядов, ИАН СССР, **10**, 35–46, 1946; Новые доказательство теоремы Гольдбаха-Виноградова, Матем. Сб., **19** (61), 3–8, 1946.

[13] L. E. Dickson, History of the theory of numbers, Vol. I. New York, 347–356, 1934.

[14] V. Brun, Le cribe d'Eratosthène et le théorème de Goldbach, Videnskabs-selskabet; Kristiania Skrifter I, Mate.-Naturvidenskapelig Klasse, **3**, 1–36, 1920.

[15] A. Selberg, On an elementary method in the theory of primes, Norske vid. selsk. Forhdl. 19, Nr. 18, 64–67, 1947.

[16] А. И. Виноградов, Новые аддитивные задачи с простыми числами, Тру. Тре. Всесоюзного Матем. Сьезда, СССР, **1**, 4, 1956.

[17] A. Selberg, The general sieve method and its place in prime number theory, Proc. of international congress of Math., **1**, 286–292, 1950.

[18] Ю. В. Линник, "Большое решета", АН СССР, **30**, 290–292, 1941.

[19] A. Rényi (А. Реньи), О представлении четных чисел в виде суммы простого и почтипростого числа, ИАН СССР, серия матем., **12**, 57–78, 1948.

[20] H. Weyl, Über die Gleichverteilung von Zahlen mod. Eins, Math. Ann., **77**, 313–352, 1916.

[21] И. М. Виноградов, О суммах Вейля, Метем, сб., **42**, 521–530, 1935.

[22] И. М. Виноградов, Избранные труды, Изд. АН СССР, Москва, 1952.

[23] 华罗庚, 堆垒素数论, 科学出版社, 1953.

[24] И. М. Виноградов, Новая оценка функции $\zeta(1+it)$, ИАН СССР, серия Матем., **22**, 161–164, 1958.

[25] E. Prouhet, Comptes Rendus, Paris, **38**, 225, 1851; 亦见 L. E. Dickson, History of the theory of numbers, Vol. **2**, New York, 705–716, 1934.

[26] 华罗庚 (L. K. Hua), On the number of solutions of Tarry's Problem, Acta Scientia Sinica, **1**, 1–76, 1953.

[27] И. М. Виноградов, Метод тригонометрических сумм в теории чисел, Тру. Матем. ии-та. Им. В. А. Стеклова, XXIII, 1947.

[28] H. Davenport, On sums of Positive integral k-th powers, Proc. Royal Soc. London (A), **170**, 293–299, 1939; On Waring's Problem for fourth powers, Ann. of Math., **40**, 731–747, 1939; On Waring's Problem for fifth and sixth powers, Amer, Journ. of Math., **64**, 199–207, 1942.

[29] Ю.В.Линник, О разложении больших чисел на 7 кубов, ДАН СССР, **36**, 179–180, 1942.

[30] L. E. Dickson, Proof of the ideal Waring theorem for exponents 7–180, Amer. Journ. Math., 58, 521–529, 1936; Solution of Waring's problem, Amer. Journ. Math., **58**, 530–535, 1936.

[31] S. S. Pillai, On Waring's problem, Journ. Indian Math. Soc. (2), **2**, 16–44, 1936; On Waring's Problem g(6)=73, Proc. Indian Acad, Sci. (A), **12**, 30–40, 1940.

[32] I. Niven, An unsolved case of Waring Problem, Amer. Journ. Math., **66**, 137–143, 1944.

[33] C. L. Siegel, Generalization of Waring's problem to algebraic number fields, Amer. Journ. of Math., **66**, 122–136, 1944.

[34] J. G. van der Corput, Neue zahlentheoretische Abschätzungen, I: Math. Ann., **89**, 215–254, 1923; II: Math. Z., **29**, 397–426, 1929.

[35] А. Я.Хинчин(A. Ja. Chinčin), Zur additiven Zahlentheorie, Матем. сб., **39**, 3, 27–32, 1932.

[36] H. B. Mann, A proof of the fundamental theorem on the density of sums of sets of positive integers, Ann. of Math. (2), **43**, 67–78, 1942.

[37] E. Artin and P. Scherk, On the sum of two sets of integers, Ann. of Math. (2), **44**, 138–142, 1943.

[38] H. H. Ostmann, Additive Zahlentheorie, Bd, I. II, Springer-Verlag, Berlin, 1956.

[39] Ю. В. Линник, Элементарное решение проблемы Waring's по методу Шнирельмана, Матем. сб.,**12** (54), 225–230, 1943.

[40] 华罗庚, 数论导引, 第十九章, 科学出版社, 1957.

[41] Н. П. Романов, К проблеме гольдбаха, Томск, Изв. ин. Матем. и тех. ун-та, I. 34–38, 1935. 亦见 Lubelski 作的文摘, 见 Zentralblatt für Math. und ihre Grenzgebiete, **11**, 390, 1935.

[42] H. Heilbronn, E. Landau und P. Scherk, Alle Grossen genzen Zahlen lassen sich also Summe von höchstens 71 Primzahlen darstellen, Časopis pro Pěstovani Math. a Fysiky **65**, 117–141, 1936.

[43] G. Ricci, Sur la congettura di Goldbach e la costante di Schnirelmann, Boll. Univ. Mat. Ital., **15**, 183–187, 1936; Annali Della R. Scuola Normale Superiore di Pisa (2) **6**, 70–115, 1937.

[44] H. Rademacher, Beiträge zur Viggo Brunschen Methode in der Zahlen-Theorie, Abh, Math. Sem. Univ, Hamburg, **3**, 12–30, 1924.

[45] T. Estermann, Eine neue Darstellung und neue Anwendungen der Viggo Brunschen Methode, J. reine angew. Math., **168**, 106–116, 1932.

[46] А. А. Бухштаб, Новые улучшения в методе эратосфенова решета, Матем, сб., **4** (46), 375–387, 1938. О разложении чётных чисел на сумму двух слагаемых с ограниченным числомпростых множителей, ДАН СССР, **29**, 544–548, 1940.

[47] A. Selberg, On elementary methods in prime number theory and their limitations, Den 11-te Skandinaviske Matematikerkongress, 13–22, 1952.

[48] H. N. Shapiro and J. Warga, On representations of large integers as sum of primes, Part. I, commun. pure appl. Math., **3**, 153–176, 1950.

[49] 尹文霖, 关于表充分大的整数为素数和, 北京大学学报 (自然科学), **3**, 323–326, 1956.

[50] И. В. Чулановский, Некоторые оченки связанные с новым методом Selberg's В элементарной теории чисел, ДАН СССР, **63**, 491–494, 1948.

[51] 王元, 整值多项式的某些性质, 数学进展, 3 卷 3 期 (1957), 416–423.

[52] P. Kuhn, Neue Abschätzungen auf Grund der Viggo Brunschen Siebmethode, Tolfte Skandinaviske Matematikerkongressen, Lund, 160–168, 1953.

[53] G. Ricci, Ricerche aritmetiche sui Polinomi, Rend, Circ. Mat. Palermo, **57**, 433–475, 1933.

[54] H. Heilbronn, Über die Verteilung der Primzahlen in Polynomen, Math. Ann., **104**, 794–799, 1931.

[55] 王元, 表大偶数为一个不超过三个素数的乘积及一个不超过四个素数的乘积之和, 数学学报, 6 卷 3 期, 500–513, 1956.

[56] 王元, 表大偶数为一个素数及一个不超过四个素数的乘积之和, 数学学报, 6 卷 4 期, 565–582, 1956.

[57] 关于素数定理的历史, 请参看第三章.

[58] A. Selberg, An elementary proof of the prime number theorem, Ann. of Math., **50**, 305–313, 1949.

[59] P. Erdös, On a new method in elementary number theory which leads to an elementary proof of the prime number theorem, Proc. Nat. Acad. Sci. USA, **35**, 374–384, 1949.

[60] Tikao Tatuzawa and Kansesiroo Iseki, On Selberg's elementary proof of the prime number theorem, Proc. Japan. Acad., **27**, 340–342, 1951.

[61] A. Selberg, An elementary proof of the prime number theorem for arithmetic progressions, Canadian J. Math., **2**, 66–78, 1950.

[62] H. N. Shapiro, On primes in arithematic progressions. I: Ann. of Math., (2) **52**, 217–230, 1950; II: Ann. of Math., (2) **52**, 231–243, 1950.

[63] W. E. Briggs, An elementary proof of a theorem about the representation of primes by quadratic forms, Canadian J. Math., **6**, 353–363, 1954.

[64] H. N. Shapiro, An elementary proof of the prime ideal theorem, Comm, Pure. Appl. Math., **2**, 309–323, 1949.

[65] W. Forman and H. N. Shapiro, Abstract prime number theorem, Comm. Pure Appl. Math., **7**, 587–619, 1954.

[66] C. F. Gauss, De nexu inter multitudinem classium etc. Werke **2**, 269–291, 1863.

[67] P. G. Lejeune-Dirichlet, Über die Bestimmung der mittleren Werte in der Zahlentheorie, Abh. Akad. Berlin (Werke **2**, 49–66) 1849, Math. Abh., 69–83.

[68] И. М. Виноградов, Основы теории чисел, М. -Л., Гостехиздат, 1944.

[69] H. Steinhaus, Sur un théorème de M. V. Jarnik, Colloquium Math., **1**, 1–15, 1948.

[70] G. H. Hardy and J. E. Littlewood, The trigonometrical series associated with the elliptic ϑ-function, Acta Math., **37**, 193–239, 1914.

[71] P. O. Кузьмин(R. O. Kusmin), Über einige trigonometrische Ungleichungen, J. Soc. Math. Phys. Leningrad, **1**, 233–239, 1927.

[72] E. Landau, Über eine trigonometrische Summe, Nachr, Ges. Wiss. Göttingen, 21–24, 1928.

[73] J. G. van der Corput, Über Weylsche Summen, Mathemtica B. 1–30, 1936–1937.

[74] J. G. van der Corput, Verschärfung der Abschätzungen beim Teilerproblem, Math. Ann., **87**, 39–65, 1922.

[75] И. М. Виноградов, О распределении дробных долей значений функций двух переменных, Изв. Ленинградского политехи ин-та, **30**, 31–52, 1927.

[76] E. C. Titchmarsh, On van der Corput's method and the zeta function of Riemann. I: Quart. J. of Math., Oxford, **2**, 161–173, 1931; II: Quart. J. of Math., Oxford, **2**, 313–320, 1931.

[77] E. Phillips, The zeta function of Riemann; Further developments of van der Corput's method, Quart. J. of Math., Oxford, **4**, 209–225, 1933.

[78] E. C. Titchmarsh, On Epstein's zeta function, Proc. London Math. Soc. (2), **36**, 485–500, 1934; The lattice points in a Circle, Proc. London Math. Soc. (2), **38**, 96–115, 1935.

[79] 闵嗣鹤 (S. H. Min), On the order of ζ $(1/2+it)$, Trans. Amer. Math. Soc., **65**, 448–472, 1949.

[80] И. М. Виноградов, Иовый метод решения некоторых общих вопросов теории чисел, Матем. сб., **43, 9–20**, 1936; Новый метод оценки тригонометрических сумм, Матем. сб., **43**, 175–188, 1936.

[81] 华罗庚 (L. K. Hua), An improvement of Vinogradov's mean value theorem and several applications, Quart. J. of Math., Oxford, **20**, 48–61, 1949.

[82] 华罗庚 (L. K. Hua), On the number of solutions of Tarry's problem, Acta Scientia Sinica, **1**, 1–76, 1952.

[83] Ю. В. Линник, (Ju. V. Linnik), On Wyel's sum, Матем. сб., **12**, 28–39, 1943.

[84] 华罗庚(Л. Т. Хуа), Аддитивная теория простых чисел, Тру. Матем. ин-та им. В. А. Стеклова, XXII, 1947.

[85] E. C. Titchmarsh, The theory of the Riemann zetafunction, Oxford, 1951.

[86] H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh, Math. Sem. Univ. Hamburg, **10**, 325–348, 1934.

[87] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Publ. Inst. Math. Strasbourg (N. S., Nr. 2), 1–85, 1948.

[88] Janichi Igusa, On the theory of algebraic correspondences and its application to the Riemann hypothesis in function fields, J. Math. Soc. Japen **1**, 147–197, 1949.

[89] P. Roquette, Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunkti- onen-körpern beliebigen Geschlechts, J. für Math., **191**, 199–252, 1953.

[90] A. Weil, Foundations of algebraic geometry, Amer. Math. Soc. Colloquium Pub., **29**, 1947.

[91] A. Weil, On some exponential sums, Proc. nat. Acad. Sci. USA. **34**, 204–207, 1948.

[92] L. Carlitz and S. Uchiyama, Bounds for exponential sums, Duke Math. J., **24**, 1, 37–41, 1957.

[93] H. D. Kloosterman, On the representation of numbers in the form $ax^2+by^2+cz^2+dw^2$, Acta Math., **49**, 407–464, 1926.

[94] H. Salié, Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen, Math. Z., **36**, 263–278, 1932.

[95] H. Davenport, On certain exponential sums, J. reine u. angew. Math., **169**, 158–176, 1933.

[96] L. J. Mordell, On a sum analogous to a Gauss's sum, Quart. J. Math., Oxford, **3**, 161–167, 1932.

[97] 华罗庚与闵嗣鹤 (L. K. Hua and S. H. Min), On a double exponential sum, Science Record, **1**, 23–25, 1942; 闵嗣鹤 (S. H. Min), On systems of algebraic equations and certain multiple exponential sums, Quart. J. Math. Oxford, **18**, 133–142, 1947.

[98] 华罗庚 (L. K. Hua), On an exponential sum, Journ. of Chinese Math. Soc., **2**, 301–312, 1940.

[99] 华罗庚 (L. K. Hua), On exponential sums over an algebraic field, Canadian J. Math., **3**, 44–51, 1951.

[100] 见华罗庚的著作 23) 与 Davenport 的著作 95)

[101] Ю. В. Линник и А. Реньи, О некоторых гипотезах теории характеров дирихле, ИАН СССР, серия Матем., **11**, 539–546, 1947.

[102] G. Pólya, Über die Verteilung der quadratischen Reste und Nichtreste, Göttingen Nachrichten, 21–29, 1918.

[103] И. М. Виноградов, О границе наименьшего невычета n-й степени, ИАН СССР, серия Матем., **20**, 47–58, 1926.

[104] N. C. Ankeny, The least quadratic non-residue, Ann. of Math., (2) **55**, 65–72, 1952.

[105] И. М. Виноградов, О наименьшем корне, ДАН СССР, 7–11, 1930.

[106] 华罗庚 (L. K. Hua), On the least primitive root of a prime, Bull. Amer. Math. Soc., **48**, 726–730, 1942.

[107] P. Erdös, On the least primitive root of a prime, Bull. Amer. Math. Soc., **51**, 131–132, 1945.

[108] P. Turán, Soviet result in number theory, Math. Lapok, 243–266, 1950.

[109] 华罗庚 (L. K. Hua), On the least solution of Pell's equation, Bull. Amer. Math. Soc., **48**, 731–735, 1942.

[110] I. Schur, Einige Bemerkungen zu drei vorstehenden Arbeiten des Herrn G. Pólya, Göttingen Nachrichten, 30–36, 1918.

[111] Ю. В. Линник(Ju. V. Linnik), On the characters of primes, I, Матем. сб., **16** (58), 101–120, 1945.

[112] R. E. A. Paley, A theorem on characters, J. London Math. Soc., **7**, 28–32, 1932.

[113] S. Chowla, On the k-Analogue of a result in the theory of the Riemann zeta function, M. Z., **38**, 483–487, 1932.

[114] P. T. Bateman, S. Chowla and P. Erdös, Remarks on the size of L(1, χ), Pub. Math., **1**, 165–182, 1950.

[115] S. Chowla, A theorem of characters, J. Indian Math. Soc., **19**, 279–284, 1932.

[116] И. М. Виноградов, Некоторые обшие теоремы относяшиеся к теории простых чисел, труды тбилисск, Матем. ин-та, **3**, 1–33, 1938; Einige allgemeine Primzahlsätze, Труды тбилисск, Матем. ин-та, **3**, 35–61, 1938. 亦可见华罗庚的著作 23).

[117] P. Turán, On Riemann Hypothesis, ИАН СССР, серия Матем., **11**, 197–262, 1947; On certain exponential sums, Proc. Akad. Wet. Amsterdam, **51**, 343–353, 1948; Eine Neue Methode in der Analysis und deren Anwendungen, Akagemiai Kiado, Budapest, 1953.

[118] И. М. Виноградов, Распределение квадратичных вычетов и невычетов вида $p+k$ попростому модулю, Матем. сб., **3**(45), 311–320, 1938; Уточнение метода оценки сумм с простыми числами, ИАН СССР, серия матем., **7**, 17–34, 1943; Новое усовершенствование методы очении двойных сумм, ДАН СССР, **73**, 635–638, 1950; Новый подход к оченке сумм значений $\chi(p+k)$, ИАН СССР, **16**, 197–210, 1952.

[119] A. M. Legendre, Essai sur la théorie des nombres, 2nd edition, Paris, 1808; Théorie des nombres, 3rd edition, Paris, 1830.

[120] C. F. Gauss, Werke **2**, 2. Aufl. Göttingen, 444–447, 1876.

[121] П. Л. Чебышев (P. L. Tschebyschev), Sur la fonction qui detérmine la totalité des nombres premiers inférieurs à une limite donnée, Memoires présentés à L'Académie Impériale des sciences des St. Pétersbourg par divers savants **6**, 141–157, 1848–1851; J. Math. pur. appl. ser. I, **17**, 341–365, 1852; CEuvres, I. 27–48, 1899; Mémoire sur les nombres premiers, Mémoires présentés à L'Académie Impériale des sciences de St. Pétersbourg par divers savants, **7**, 15–33, 1850–1854; J. Math. pur. appl. ser. I, **17**, 366–390; 1852; CEuvres, **1**, 49–70, 1899.

[122] J. J. Sylvester, On Tschebyschev's theory of the totality of Prime numbers comprised within given limits, Amer. J. Math., **4**, 230–247, 1881.

[123] B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Größe, Ges. Math. Werke und Wissenschaftlicher Nachlaß, 2. Aufl., 145–155. 1892.

[124] J. Hadamard, Essai sur l'étude des fonctions données par leur développement de Taylor, J. Math. pur. appl. (4), **8**, 101–186, 1892; Etude sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann, J. Math. pur. app. (4), **9**, 171–215, 1893.

[125] J. Hadamard, Sur la distribution des zéros de la fonction $\zeta(s)$ et des conséquences arithmétiques, Bull. Soc. Math. France **24**, 199–220. 1896.

[126] C. J. de la Vallée Poussin, Recherches analytiques sur la théorie des nombres, premièrepartie: La fonction $\zeta(s)$ de Riemann et les nombres. premiers en général, Ann. Soc. Sci. Bruxelles **20**, 183–256, 1896.

[127] H. von Mangoldt, Auszug aus einer Arbeit unter dem Titel: Zu Riemanns Abhand-

lung “Über die Anzahl der Primzahlen unter einer gegebenen Größe”, Sitzungsber, d. Preuss. Akad. d. Wiss. 883–896, 1894; Zu Riemanns Abhandlung “Über die Anzahl der Primzahlen unter einer gegebenen Größe”, J. reine u. angew. Math. **144**, 255–305, 1895. Zur Verteilung der Nullstellen der Riemannschen Funktion $\xi(t)$, Math. Ann., **60**, 1–19, 1905.

[128] R. J. Backlund, Sur les zéros de la fonction $\zeta(s)$ de Reimann, Comptes, Rendus, **158**, 1979–1981, 1914; Über die Nullstellen der Riemannschen Zetafunktion, Acta Math., **41**, 345–375, 1918.

[129] H. von Koch, Sur la distribution des nombres premiers, Acta Math., **24**, 159–182, 1901.

[130] C. J. de la Vallée. Poussin, Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premiers inférieurs á une limite donnée, Mémoires couronnes de l'Acad. Roy. des Sci. de Belgique **59**, Nr. 1. 1899–1900.

[131] J. E. Littlewood, Researches in the theory of Riemann ζ-function, Proc. London Math. Soc. (2), **20**, XXII-XXVIII, 1922.

[132] Н. Г. Чудаков (J. G. Tschudakov), on zeros of Dirichlet's L-functions, Матем. сб., **1** (43), 591–602, 1936; О функпиях $\zeta(s)$ и $\pi(x)$, ДАН СССР, 425–426, 1938.

[133] E. C. Titchmarsh, On $\zeta(s)$ and $\pi(x)$, Quart. J. Math. Oxford, **9**, 97–108, 1938.

[134] B. Rosser, The n-th prime is greater than $n \log n$, Proc. London Math. Soc. (2), **45**, 21–44, 1938; Explicit bounds for some functions of prime numbers, Amer. J. Math. **63**, 211–232, 1941.

[135] A. E. Ingham, The distribution of prime numbers, Cambridge tracts, **30**, 1932.

[136] J. E. Littlewood, Sur la distribution des nombres Premiers, Comptes Rendus, **158**, 1869–1872, 1914.

[137] S. Skewes, On the difference $\pi(x)$-lix I: J. London Math. Soc., 8, 277–283, 1933; II: Proc. London Math. Soc., (3) 5, 48–70, 1955, 亦可参考 A. E. Ingham, A note on the distribution of Primes, Acta Arith., **1**, 201–211, 1936.

[138] E. Schmidt, Über die Anzahl der Primzahlen unter gegebener Grenze, Math. Ann., **57**, 195–204, 1903.

[139] G. Pólya, Über das Vorzeichen des Restgliedes im Primzahlsatz, Gött. Nachr. 19–27, 1930.

[140] 参看 J. E. Littlewood 的文章 136), 亦可参看 E. Landau, Vorlesungen über Zahlentheorie, Leipzig, 11, 123–150, 1927 或 A. E. Ingham, A note on the distribution of primes, Acta Arith, I. 201–211, 1936.

[141] A. E. Ingham, On the difference between consecutive primes, Quart. J. Math., Oxford, **8**, 255–266, 1937. 该文的方法已被 Fogels 用来处理数论函数和各种问题, 见 On average value of arithmetic functions, Proc. Cambridge Phil. Soc., **37**, 358–372, 1941.

[142] H. Cramér, Some theorems concerning prime numbers, Arkiv för Mat., Astr. och Fys. **15**, 5, 1921.

[143] R. A. Rankin, The difference between consecutive prime numbers, J. London math. Soc., **13**, 242–247, 1938. 同时参考 E. Westzynthius, Über die Verteilung der zahlen, die zu den ersten Primzahlen teilerfremd sind, Commentationes Phys.-mat. Soc. Sci. fenn. **5**, Nr. 25, 1–37, 1931. P. Erdös, On the difference of consecutive primes, Quart. J. Math., Oxford, **6**, 124–128, 1935. 张德馨 (T. H. Chang), Über aufeinanderfolgende Zahlen, von denen jede mindestens einer von n linearen Kong-ruenzen genügt, deren Moduln die ersten n Primzahlen sind. Schriften Math. Sem. u. Inst. Angew. Math. Univ., **4**, 35–55, 1938.

[144] A. E. Western, Note on the magnitude of the difference between successive primes, J. Lon-don math. Soc., **9**, 276–278, 1934.

[145] R. A. Rankin, The difference between consecutive prime numbers, II: Proc. Cambridge philos. Soc., **36**, 255–266, 1940; The difference between consecutive prine numbers, III: J. London math. Soc., **22**, 226–230, 1947; The difference between consecutive prime numbers, IV: Proc. Amer. math. Soc., **1**, 143–150, 1950; P. Erdös, The difference of consecutive primes, Duke math. J., **6**, 438–441. 1940.

[146] O. Ricci, Sull'andamento della differenza di numeri primi consecutivi, Rev. Math. Univ. Parma, **5**, 3–54, 1954.

[147] A. Walfisz (А. З. Вальфиш), Изолированные простые числа, ДАН СССР, **90**, 711–713, 1953.

[148] K. Prachar, Über ein Resultat von A. Walfisz, Monatsh. Math., **58**, 114–116, 1954.

[149] H. Cramér, On the order of magnitude of the difference between consecutive prime numbers, Acta Arith., **2**, 23–46, 1936.

[150] A. Selberg, On the normal density of primes in small intervals, and the difference between consecutive primes, Arch. Math. Naturvid., **47**, 87–105, 1943.

[151] G. Hoheisel, Primzahlprobleme in der Analysis, Sitzungsber. der Preuß. Akad. d. Wissensch., Phys.-Math. Kl. Berlin, 580–588, 1930.

[152] H. Heilbronn, Über den Primzahlsatz von Herrn Hoheisel, Math. Z. **36**, 394–423, 1933.

[153] Н. Г. Чудаков (N. Tchudakoff), On the difference between two neighbouring prime numbers, Матем. сб., **1**(43), 793–814, 1936.

[154] P. Turán, Eine neue Methode in der Analysis und deren Anwendungen, Akadémial Kiadó, Budapest 1953. (有中译本, "数学分析中的一个新方法及其应用", 郭焕庭译, 见数学进展, 第二卷, 312–365, 1956).

[155] H. Cramér, On the order of magnitude of the difference between consecutive prime numbers, Proc. mat-fiz., **45**, 51–74, 1937; Acta math., **2**, 23–46, 1936.

[156] И. Г. Чудаков, О конечной разности для функции $\varphi(x, k.l)$, ИАН СССР, сер-

ия матем., **12**, 31–49, 1948; К. А. Родосский, О распределении простых чисел в коротких арифметических прогрессиях. ИАН СССР, серия матем., **12**, 123–128, 1948.

[157] A. Page, On the number of primes in an arithmetic progression, Proc. London math. Soc. (2) **39**, 116–141, 1935.

[158] Tikao Tatuzawa, On the number of the primes in an arithmetic progression, Japanese J. Math., **21**, 93–111, 1951.

[159] C. L. Siegel, Über die Klassenzahl quadratischer Zahlkörper, Acta Arith., **1**, 83–86, 1936.

[160] A. Walfisz, Zur additiven Zahlentheorie II, Math. Z., **40**, 592–607, 1936.

[161] Ю.В.Линник (U. V. Linnik); On the least prime in an arithmetic progression, I: The basic theorem, Матем. сб., **15** (57), 139–178, 1944; II: The Deuring-Heibronn's phenomenon, Матем. сб., **15** (57), 347–368, 1944.

[162] К. А. Родосский, О наименьшем простом числе в арифметической прогрессии и нулях L-функций, ДАН СССР, **88**, 753–756, 1953; О наименьшем простом числе в арифметической прогрессии, Матем, сб., **34** (76), 331–356, 1954.

[163] S. Chowla, On the least prime in an arithmet. Progression, J. Indian math. Soc., **1**, 1–3, 1934.

[164] P. Turán, Über die Primzahlen der arithmetischen Progression, Acta Litt. Sci. Szeged **8**, 226–235, 1937.

[165] P. Erdös, On some applications of Brun's method, Acta Univ. Szeged. Sect. Sci. Math., **13**, 57–63, 1949.

[166] Hans-Egon Richert, Über quadratfreie Zahlen mit genau t Primfaktoren in einer arithmetischen Progression, J. reine u. angew. Math., **192**, 180–203, 1953.

[167] И. И. Пятецкий-Шапиро, О распределении простых чисел в последовательностях вида $|f(n)|$, Матем. сб., **33** (75), 559–566, 1953.

[168] E. Landau, Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes, Math. Ann., **56**, 645–670, 1903; Über ideale und Primidale in Idealklassen, Math. Z., **2**, 52–154, 1918.

[169] А. А. Бухштаб, Асимптотическая оценка одной общей теоретико-числовой функции, Матем. сб., **2**, 1239–1245, 1937.

[170] S. Chowla and T. Vijayaraghaven, On the largest prime divisors of numbers, J. Indian math. Soc., **11**, 31–37, 1947.

[171] А. А. Бухштаб. О числах арифметической прогрессии у которых все простых множители малы по порядку роста, ДАН СССР, **67**, 5–8, 1949.

[172] 华罗庚 (L. K. Hua), 一个求极限的问题, 中国科学, **2**, 393–402, 1951.

[173] 闵嗣鹤 (S. H. Min), 谈一个求极限的问题, 数学学报, **8**, 381–384, 1954.

[174] N. G. de Bruijn, On the number of uncancelled elements in the sieve of Eratosthenes, Indag. math., **12**, 247–256, 1950; The asymptotic behaviour of a function occurring in the theory of primes, J. Indian math. Soc., **15**, 25–32, 1951.

[175] А. А. Бухштаб, Об асимптотической оценке числа чисел арифметической прогрессии неделящихся на"относительно"малые простые числа, Матем. сб., **28** 165–184, 1951.

[176] N. G. de Bruijn, On the number of positive integers $\leqslant x$ and free of prime factors $> y$, Nederl. Akad. Wet., Proc., Ser. A 54, 50–60, Indagat. math., **13**, 50–60, 1950. 同时参考 Ramaswami, The number of positive integers $\leqslant x$ and free of prime divisors $> x^c$ and a problem of S. S. Pillai, Duke math. J., **16**, 99–109, 1949; Number of integers in a assigned A. P., $\leqslant x$ and prime to primes greater than x^c, Proc. Amer. math. Soc., **2**, 318–319, 1951.

[177] 华罗庚 (L. K. Hua), On Waring's problem, Quart. J. Math., Oxford, **9**, 199–202, 1938.

[178] 这个结果稍优于Вивогродов 原来的结果: $s \geqslant [10\ k^2 \log k]$.

[179] P. Erdös, On the representation of an integer as the sum of k k-th powers, J. London math. Soc., **11**, 133–136, 1936.

[180] S. Chowla and S. S. Pillai, The number of representations of a number as a sum of n nonnegative *n-th* powers, Quart. J. Math., Oxford, **7**, 56–59, 1936.

[181] K. Mahler, Note on hypothesis K of Hardy and Littlewood, J. London math. Soc., **11**, 136–138, 1936.

[182] G. L. Watson, A proof of the seven cube theorem, J. London math. Soc., **26**, 153–156, 1951.

[183] 例如 F. Hausdorff, Math. Ann., **67**, 301–305, 1909; E. Stridsberg, Math. Ann., **72**, 145–152, 1912.

[184] 华罗庚 (L. K. Hua), On a generalized Waring problem, Proc. London. Math. Soc. (2), **43**, 161–182, 1937.

[185] R. E. Huston, Asymptotic generalizations of Warings theorem, Proc. London math. Soc., **39**, 82–115, 1935.

[186] 华罗庚 (L. K. Hua), On Waring problem with polynomial summands, Amer. J. Math., **58**, 553–562, 1936; On a generalized Waring problem, Proc. London math. Soc. (2) **43**, 161–182, 1937; On a generalized Waring problem, II, Journ. Chinese Math. Soc. (2), 175–191, 1940.

[187] 华罗庚 (L. K. Hua), On Waring problem with cubic polynomial summands, J. Indian math. Soc., **4**, 127–135, 1940.

[188] В. И. Нечаев, О представлении натуральных чисел суммой слагаемых вида $\frac{x(x+1)\cdots(x+k-1)}{k!}$, ИАН СССР, **17**, 485–498, 1953.

[189] 华罗庚 (L. K. Hua)[23], 同时参考 S. S. Pillai, On Warings problem VI (polynomial summands), J. Annamalai Univ., **6**, 171–197, 1937.

[190] K. F. Roth, A problem in additive number theory, Proc. London math. Soc. (2) **53**, 381–395, 1951.

[191] E. M. Wright. An extension of Warings problem Philos. Trans. Roy. Soc. London **232**, 1–26, 1933; Proportionality conditions in Warings problem, Math. Z **38**, 730–746, 1934.

[192] F. C. Auluck and S. Chowla, The representation of a large number as a sum of "almost equal" squares, Proc. Indian Acad. Sci., Sect. A. **6**, 81–82, 1937; 同时参考 E. M. Wright, The representation of a number as a sum of four "almost proportional" squares, Quart. J. Math. Oxford, **7**, 230–240, 1936.

[193] Б. И. Сегал, Об одной теореме, аналогичной теореме Варинга, ДАН СССР, Новая серия, **2**, 47–49, 1933.

[194] S. Chowla, A theorem on irrational indefinite quadratic forms, J. London math. Soc. **9**, 162–163, 1934.

[195] H. Davenport and H. Heilbronn, On indefinite quadratic forms in five variables, J. London math. Soc. **21**, 185–193, 1946.

[196] H. Davenport and K. F. Roth. The solubility of certain Diophantine inequalities, Mathematica **2**, 81–96, 1955.

[197] A. Oppenheim, Values of quadratic forms, III. Monatsh. Math. **57**, 97–101, 1933.

[198] L. E. Dickson, Recent progress on Waring theorem, Bull. Amer. math. Soc. **39**, 701–727, 1933.

[199] S. S. Pillai, Waring's problem with indices $\geqslant n$, Proc. Indian, Acad. Sci. (A) **12**, 41–45, 1940. 同时参考 M. Haberzetle, The Waring problem with summands $x^m, m \geqslant n$, Duke math. J. 5, 49–57, 1939.

[200] E. M. Wright, On Tarry's problem, Quart. J. Math., Oxford, **6**, 261–267, 1935.

[201] 华罗庚 (L. K. Hua), On Tarry's problem, Quart. J. Math., Oxford, **9**, 315–320, 1938. 同时参考 E. M. Wright, On Tarry's problem III. Quart J. Math., Oxford, **8**, 48–50, 1937.

[202] 华罗庚 (L. K. Hua), Improvement of a result of Wright, J. London Math. Soc. **24**, 157–159, 1943.

[203] К. К. Марджанишвили, Об одновременном представлении и чисел суммами полных первых, вторых,$\cdots n$-ых степеней, ИАН СССР, серия матем., **1**, 609–631, 1937; О некоторых нелинейных системах уравнений в целых числах, Матем. сб., **33**, 639–675, 1953.

[204] T. Estermann, A new result in the additive prime-number theory, Quart. J. Math., Oxford, 8, 32–38, 1937.

[205] T. Estermann, Proof that every large integer is the sum of two primes and a square, Proc. London math. Soc. **11**, 501–516, 1937.

[206] Ю.В. Линник, О возможности единого метода в некоторых вопросах “аддитивной”н “дистрибутивной”теории простых чисел, ДАН СССР, **49**, 3–7, 1945.

[207] Н. Г. Чудаков (N. Tchudakoff), On Goldbach-Vinogradov's theorem, Ann. of Math. (2) **48**, 515–545, 1947.

[208] C. B. Haselgrove, Some theorems in the analytic theory of numbers, J. London Math. Soc. **26**, 273–277, 1951.

[209] R. D. James and H. Weyl, Elementary note on prime-number problems of Vinogradov's type, Amer. J. Math. **64**, 539–552, 1942.

[210] Hans-Egon Richert, Aus der additiven Primzahltheorie, J. für Math. **191**, 179–198, 1953.

[211] J. G. Van der Gorput, Propriétés additives, Acta Arithm. **3**, 181–234, 1939.

[212] A. Zulauf, Beweis einer Erweiterung des Satzes von Goldbach-Vinogradov, J. reine angew. Math. **190**, 169–198, 1952.

[213] 吴方 (Wu Fang), 素数变数的线性方程组, 数学学报, **7**, 102–121, 1957.

[214] J. G. Van der Corput, Sur l'hypothese de Goldbach pour presque tous les nombres pairs, Acta Arithm. **2**, 266–290, 1937.

[215] И. Г. Чудаков, О проблеме гольдбаха, ДАН СССР, **17**, 331–334, 1937.

[216] T. Estermann, Proof that almost all even positive integers are sums of two primes, Proc. London math. Soc. (1) **44**, 307–314, 1938.

[217] H. Heibronn, 见 Zentralblatt für Mathematik und ihre Grenzgebiete, **16**, 291–292, 1937.

[218] 华罗庚 (L. K. Hua), Some results in the additive prime number theory, Quart. J. Math., Oxford, **9**, 68–80, 1938.

[219] Ю.В. Линник, Некоторых уисловные теоремы, касающиеся бинарных задач с простыми числами, ДАН СССР, **77**, 15–18, 1951; Некоторых условные теоремы касающиеся бинарной проблемы Гольдбаха, ИАН СССР, **16**, 503–520, 1952.

[220] Ю.В. Линник, Складывание простых чисел со степенями одного и того же числа, Матем. сб., **32**, 3–60, 1953.

[221] А. А. Бухштаб, Об одном аддитивном представлении целых чисел, Матем. сб., **10**, (52), 1–2, 87–91, 1942.

[222] 华罗庚 (L. K. Hua)[23] 也见И. М. Виноградов, Einige allgemeine Primzahisätze. Труды Тбилисск. Матем. Института, **3**, 35–67, 1938; 华罗庚, On the representation of numbers as the sum of powers of primes, Math. Z. **44**, 335–346, 1938; S. Pillai, On Waring's problem with powers of primes, Proc. Indian Acad. Sci., Sect. A **12**, 202–204, 1940.

[223] H. Halberstam, Representation of integers as sums of a square of a prime and a cube of a prime and a cube, Proc. London math. Soc. (2) **52**, 455–466, 1951.

[224] K. Prachar, Über ein problem vom Waring-Goldbachschen Typ. I. Monatsh. Math. **57**, 66–74, 1953; Über ein problem vom Waring-Goldbachschen Typ. II, Monatsh. Math. **57**, 113–116, 1953.

[225] И. И. Шапиро-Пятецкий, Об одном варианте проблемы Варинга-Гольдбаха, Матем. сб., **30**, 105–120, 1952.

[226] К. К. Марджанишвили, Об одной задаче аддитивной теории чисел, ИАН СССР., серия матем., **4**, 193–214, 1940.

[227] J. G. Van der Corput, Diophantisch Ungleichungen I, zur Gleichverteilung modulo Eins, Acta math., **56**, 373–456, 1931.

[228] I. F. Koksma, Ein mengentheoretischer Satz über die Gleichverteilung modulo Eins, Compositio math., **2**, 250–258, 1935.

[229] И. М. Виноградов, Аналитическое доказательство теоремы о распределении дробных частей целого многочлена, ИАН СССР, серия матем. (6), **21**, 567–578, 1927.

[230] I. F. Koksma, Diophantische Approximationen, Springer-Verlag, Berlin 1936.

[231] P. Erdös and P. Turán, On a problem in the theory of uniform distribution, I. Proc. Akad. Wet. Amsterdam 1146–1154, 1948.

[232] T. Van Aardenne-Ehrenfest, On the impossibility of a just distribution, Proc. Akad. Wet. Amsterdam **52**, 734–739, 1949.

[233] И. М. Виноградов, Об оценке тригонометрических сумм с простыми числами, ИАН СССР, серия матем., **12**, 225–248, 1948.

[234] P. Turán, Über die Primzahlen der arithmetischen Progression, Acta Litt. Sci. Szeged **8**, 226–235, 1937.

[235] А. Г. Постников, К вопросу о распределении дробных долей показателъной функции, ДАН СССР, **86**, 473–476, 1952; И. И. Шапиро-Пятечкий, О законах распредерения дробных долей показателъной фуикции, ИАН СССР, Серия матем. **17**, 49–52, 1951.

[236] Н. М. Коробов, О некоторых вопросах равномерного распределения, ИАН СССР, серия матем., **14**, 215–238, 1950.

[237] Н. М. Коробов, Многомерные задачи распределения дробных долей, ИАН СССР, серия матем., **17**, 389–400, 1953; Дробные доли показателъных функчий, Труды матем. института им. Стеклова. АН СССР, **38**, 87–96, 1951; О дробных долях показателъных функций, УМН, СССР, **6**, 151–152, 1951.

[238] E. Landau, Über die Anzahl der Gitterpunkte in gewissen Bereichen, Gött. Nachr. 687–771, 1912.

[239] A. Oppenheim, Some identities in the theory of numbers, Proc. London math. Soc. (2) **26**, 295–350, 1927.

[240] V. Jarnik, Über Gitterpunkte in der Ebene, Rozpravy **33**, 36, 1924.

[241] Г. Вороной (G. Voronoi), Sur un problème du calcul des fonctions asymptotiques, J. für Math. **126**, 241–282, 1903.

[242] W. Sierpinski, O pewnem zagadnienise z rachunku funkcyi asymptotycznych, Prace Mat.-Fisz. **17**, 77–118, 1906.

[243] I. E. Littlewood and A. Walfisz, The lattice points of a circle, Proc. Royal Soc. London, Ser. (A) **106**, 478–488, 1925.

[244] A. Walfisz, Teilerprobleme, Math. Z. **26**, 66–88, 1927.

[245] L. W. Nieland, Über das Kreisproblem, Math. Ann. **98**, 717–736, 1928.

[246] 华罗庚 (L. K. Hua), The lattics points in a circle, Quart. J. Math., Oxford, **13**, 18–29, 1942.

[247] I. G. Van der Corput. Zum Teilerproblem, Math. Ann. **98**, 697–716, 1928.

[248] 迟宗陶 (T. T. Chih), The Dirichlet's divisor problem, Science Report of Tsing Hua Univ., 402–427, 1950.

[249] H. E. Richert, Verschärfung der Abschätzung beim Dirichletschen Teilerproblem Math. Z. 58, 204–218, 1953.

[250] G. H. Hardy, On Dirichlet's divisor problem, Proc. London math. Soc. **15**, 1–25, 1916.

[251] A. E. Ingham, On the classical lattice point problems, Proc. Cambridge philos. Soc. **36**, 131–138, 1940. P. Erdös 与 W. H. J. Fuchs 用一初等方法得到了一个精确性稍差但更一般的结果, 见 On a problem of additive number theory, Lond. Math. Soc. **31**, 67–73, 1956.

[252] E. Landau, Über die Gitterpunkte in einem Kreise IV, Gött. Nachr., 58–65, 1924.

[253] 董光昌 (K. C. Tong), 除数问题 (III), 数学学报, **6**, 515–541, 1956.

[254] G. H. Hardy and I. E. Littlewood, The approximate functional equation in the theory of the zeta-function, with applications to the divisor problems of Dirichlet and Piltz, Proc. London math. Soc. (2) **21**, 39–74, 1922.

[255] 董光昌 (K. C. Tong), 除数问题, 数学学报, **2**, 258–266, 1952.

[256] F. V. Atkinson, A divisor problem, Quart. Journ. Math. (Oxford), **12**, 193–200, 1941.

[257] E. C. Titchmarsh, On divisor problems, Quart. J. Math., Oxford, **9**, 216–220, 1938.

[258] H. Cramér, Über das Teilerproblem von Piltz, Arkiv für Mat., Astr. och Fysik **16**, 21, 1922.

[259] E. Landau, Zur analytischen Zahlentheorie der definiten quadratischen Forman (Über die Gitterpunkte in einem mehrdimensionalen Ellipsoid), Berliner Akademieberichte, 458–476, 1915. Über eine Aufgabe aus der Theorie der quadratischen Forman, Wiener Akademieberichte, **124**, 445–468, 1915. Über die Anzahl der Gitterpunkte in gewissen Bereichen IV, Gött. Nachr., 137–150, 1924.

[260] A. Walfisz, Über Gitterpunkte in mehrdimensionalen Ellipsoiden, Math. Z. **19**, 300–307, 1924.

[261] E. Landau, Über Gitterpunkte in mehrdimensionalen Ellipsoiden, Math. Z. **21**, 126–132, 1924.

[262] V. Jarnik, Über die Mittelwertsätze der Gitterpunktlehre I, Math. Z. **33**, 62–84, 1931.

[263] A. Walfisz, Über Gitterpunkte in mehrdimensionalen Ellipsoiden, VIII, Acad. Sci. URSS. Trav. Inst. math. Thilissi, **5**, 181–196, 1939.

[264] 这个结果能用Виноградов[24)] 的方法证得.

[265] V. Jarník, Über die Mittelwertsätze der Gitterpunktlehre, V. Casopis Mat. Fysik., Praha, **69**, 148–174, 1940.

[266] И. М. Виноградов, Число целых точек в шаре, Труды Матем. Института им. В. А. Стеклова, **9**, 17–38, 1935.

[267] И. М. Виноградов, Улучшение остаточного члена одной асимптотической формулы, ИАН СССР, серия матем., **13**, 97–110, 1949.

[268] И. М. Виноградов, Улучшение асимптотических формул для числа целых точек в области трех измерений, ИАН СССР, серия матем., **19**, 3–9, 1955.

[269] G. Szegö, Beiträge zur Theorie der Laguerreschen Polynome II, Zahlentheoretische Anwendungen, Math. Z. **25**, 388–404, 1926.

[270] Ю. В. Линник, Асимптотическое распределение целых точек на сфере, ДАН СССР, **96**, 909–912, 1954.

[271] А. В. Малышев, Асимптотическое распределение целых точек на некоторых эллипсоидах, труды третьего всесоюзного математического съезда АН СССР, 7–8, 1956.

[272] H. Davenport and K. F. Roth. On the gaps between consecutive k-free integers, J. London math. Soc. **26**, 268–273, 1951.

[273] H. E. Richert, On the difference between consecutive squarefree numbers, J. London math. Soc. **29**, 16–20, 1954, 同时参考 K. F. Roth, On the gaps between square-free numbers, J. London Math. Soc. **26**, 263–268, 1951.

[274] R. Erdös, Some problems and results in number theory, Publ. Math. Debrecen, **2**, 103–109, 1951.

[275] 由于相似性, 故未将学生素数问题的结果列入表内.

《华罗庚文集》已出版书目

（按出版时间排序）

1 华罗庚文集数论卷 I 王元 审校 2010 年 5 月
2 华罗庚文集数论卷 II 贾朝华 审校 2010 年 5 月
3 华罗庚文集数论卷 III 王元 潘承彪 贾朝华 审校 2010 年 5 月
4 华罗庚文集代数卷 I 万哲先 审校 2010 年 5 月
5 华罗庚文集多复变函数论卷 I 陆启铿 审校 2010 年 5 月
6 华罗庚文集应用数学卷 I 杨德庄 主编 2010 年 5 月
7 华罗庚文集应用数学卷 I 杨德庄 主编 2010 年 5 月
8 华罗庚文集代数卷 II 待定
9 华罗庚文集多复变函数论卷 II 待定